The front lines in the war against cyber threats is a battle that should not and cannot be faced alone. The threat landscape is evolving too fast, the sophistication of attacks are increasing too rapidly, and the sheer volume of threats is long past being too overwhelming for any one company to handle on their own.

In 2014, we emphasized the importance of data and information sharing. Over the past year, we have observed a radical increase in sharing initiatives, willingness to share data, and the general acceptance that we need to work together to stay ahead of our common adversaries.

We can’t stop here though. In the war against cyber criminals, we’re all on the same team. We need to continue to exchange experiences, share knowledge, and collaborate internationally amongst the security community, law enforcement, governments and enterprises.

Last year, we announced a data exchange program with Europol. This year, we’re going further to lead the team. Over the past year this has included:

- Sharing our insight into the war on cybercrime at the George C. Marshall European Center for Security Studies
- Research participation in Ars Forensica, an initiative to create an international standard for digital forensics led by Center for Cyber and Information Security, with contribution from United Nations Interregional Crime and Justice Research Institute, Europol Cybercrime Center (EC3), National Criminal Investigation Service Norway (Kripos), and others
- Research contribution to Oslo Analytics, a joint research project at the University of Oslo to develop solutions for holistic analysis of cybersecurity incidents, and organized in collaboration with the US Army Research Labs, the Norwegian Defence Intelligence College (FEH), the Norwegian National Security Authority (NSM), Technical University of Darmstadt and others
- Expanding data sharing agreements to include Norwegian Cyber Defence Force (Cyberforsvaret) and KraftCERT – Norway’s national Computer Emergency Response Team for the energy sector
- Launching our free SecureDNS service for corporate and home users

mnemonic will continue to invest in research activities and security initiatives that give back to the security community and enable collaboration in combining our efforts against cyber criminals. We encourage our partners, customers, colleagues and competitors to do the same, and to join us in our collaborative war against cyber crime.

Interested in collaborating and joining the fight against cyber crime? Send an email to JoinTheTeam@mnemonic.no and join the team!

Tønnes Ingebrigtsen

CEO at mnemonic as

JOIN THE TEAM
TABLE OF CONTENTS

Evolving from detection to prediction – the state of R&D in mnemonic 5

There’s no such thing as security 7

Measuring Cybersecurity Culture: Is it possible to create a standardized metric? 11

Security Predictions – 2016 and beyond 13

Predicting future trends in the arms race against cybercriminals 17

SSL, TLS, WTF! Secure crypto in 2016 21

How can you manage risks you don’t know about? 25

Vulnerable to vulnerabilities – how do we keep up? 29

Application security in a self-service world 33

Securing Industrial Control Systems with Software-Defined Networking 37
As cyber criminals continue to evolve, so too must our defenses, and thereby our capabilities as a security vendor. Traditionally, criminals have come up with new techniques, methods and strategies and the security industry experts have countered. It is an ongoing game of cat and mouse.

At mnemonic, we aim to change the game. We want to move ahead of the curve and evolve from just detecting threats to predicting them. Our ambitions are to predict the threats you will face, anticipate the attackers' next move and mitigate the threat before it becomes a reality.

We want to continue to influence the way this industry moves forward. A large part of this effort is through contributing to research and offering insights in our areas of expertise - areas that will be of value to our customers and partners in the future.

SHARING IS CARING

Getting there means hard work, innovation and great minds, and we know we can’t accomplish it entirely on our own. Traditionally, threat intelligence and this kind of research have been safeguarded well within the protective walls of the different security companies. With the ambitious goals we have set, we need to change the way we collectively face cyber threats.

Sharing knowledge, experience and threat intelligence by working together with some of the best researchers and institutions is one of the keys to move the industry ahead.

We believe sharing is one of the keywords for the industry going forward. The other two are “research” and “development”.

A GLIMPSE INTO MNEMONIC R&D

In last year’s report, we introduced some of our sharing and collaboration efforts, such as those with Europol, Check Point and Norway’s FinansCERT. This year, we’re shining the spotlight on a selection of the research projects mnemonic are involved in.

After 15 years in the security industry, we accumulated priceless experiences and have much to offer in contributing to security research projects. Our involvement in research programs, attending events such as the 3rd Interpol - Europol - cybersecurity conference and speaking at the Marshall Center in Garmisch-Partenkirchen keeps us on our toes and contributes vastly to our competency and expands our professional network.
RESEARCH PARTNERSHIPS

Ars Forensica

mnemonic is a partner in Ars Forensica, a research project focusing on developing a new international standard for data forensics. The project is funded by the Ministry of Justice and Public Security and the Research Council of Norway, and is run by the Center for Cyber and Information Security and the National Police Directorate. Also participating in the project are the United Nations Interregional Crime and Justice Research Institute and the Europol Cybercrime Center.

Being a part of Ars Forensica means that we are evolving our competency, our toolkit and our services by working together with some of the brightest minds in the industry. The goal is to find new tools to investigate cybercrime – tools that need to find relevant clues in vast amounts of data.

Oslo Analytics

At the University of Oslo, mnemonic is a partner in the Oslo Analytics project. The goal of the research is to develop solutions for holistic analysis of cybersecurity incidents. Using big data analysis, subjective logic and Bayesian modelling, the project develops advanced analytical methods to gain a deep situational awareness and understanding of security incidents. The project is organized in collaboration with the US Army Research Labs, the Norwegian National Security Authority (NSM), the Norwegian Computing Center, the Defence Intelligence College, and TU Darmstadt.

A SNEAK PEEK AT MNEMONIC’S INTERNAL R&D

Adaptive Malware Analysis & Deconstruction

Malware is dynamic and evolving, and thanks to easy to use and well supported exploit kits, tens to hundreds of thousands of new malware samples are being created every day. Besides being unrealistic, it’s a losing battle to create signatures for each new sample. However when malware is deconstructed, the vast majority originate from a few core families that share structural design and functionality. By combining deconstructed malware analysis, execution behavior, heuristics, reputation and dynamic identifiers, we can identify unknown malware – automatically and in real-time.

Machine Learning & Predictive Analytics

At a basic level, machine learning is the principle of teaching computers to act without being explicitly told what to do. Modern uses include speech recognition, self-driving cars and search optimization. mnemonic is applying the principles of machine learning to our Argus platform in several ways to support our advanced threat defense efforts.

When identifying threats, the complexity and sheer amount of data to be analysed is accelerating. Machine learning enables us to use this to our advantage in identifying new threats that have not yet been seen before, and be even more precise in our threat detection of those that are known to us. We are then taking this a step further with predictive analytics to anticipate future threats.

Defending against cyber threats is as much about interpreting the context as it is about identifying the threat in the first place. Without context, a threat is merely an event in time. Context is what makes us understand the who, the what, the how and the why – all necessary details needed to discern the consequences, business impact and appropriate response.

Today, we rely on humans to add this context, and we will continue to do so for the foreseeable future. The more we can train Argus to make routine decisions, the more we can free up analyst “brain time” for the complex decisions and deriving of context that require human interpretation.

GETTING TO THE FUTURE

These are just a glimpse at some of the R&D activities mnemonic is participating in. These are all in addition to our open security services, such as our free PassiveDNS and SecureDNS services, and other open initiatives we’re sponsoring, like URLQuery.net, and providing financial backing to a handful of other projects.

The future is an interesting place – and we are keen on getting there as soon as possible.
There's No Such Thing As Security

Written by: Jan Henrik Schou Straumsheim, Senior Security Analyst

After reading this article, you will:

• Know why practice and knowledge can not be replaced by technology alone
• Understand that we need knowledge to truly understand and solve problems
• Understand that theoretical plans are worthless without a practiced team

As of late, I've been pondering the idea that perfect security is unattainable. Some say there is no such thing as security, while others claim that there are only varying degrees of uncertainty. The notion that whatever you're doing does not provide any real security is an uncomfortable thought. On the other hand, I'm sure most professionals agree that the idea of perfect security is naive at best.

If we elaborate, perhaps we can agree that most companies are struggling with varying degrees of (in)security. How we manage risk depends on a variety of factors: Our overall preparedness, level of training, appetite, luck, and so forth. Security does not have to be perfect in order to be beneficial. On the other hand, risks have to be manageable and/or acceptable. Some businesses understand this better than others. For example, credit card companies like Visa and MasterCard lose billions of dollars on fraud every year, but you are unlikely to see them going out of business anytime soon.

On the topic of managing risks, here's a story that explains the situation many of my security colleagues face on a daily basis:

A man is driving his car on his way home from work. Pulling into to his driveway, he can immediately tell something is wrong. He steps out of the car and walks up to the front door, which is wide open. He peeks inside, only to see that his furniture is shattered and drawers have been ripped opened. The place looks like a mess. It’s obviously a burglary. Confused and afraid, the man walks outside. He stops on his lawn when he spots another man sitting in a reclining armchair on the other side of the street. Curious, he walks over and asks:

"Excuse me, Sir, do you know what happened?"

The man in the chair replies: “Yeah, sure! Your house was robbed while you were away. It probably happened because you hadn’t locked your door, and the burglar alarm never rang”.

The man who’s just been robbed looks at him, raising an eyebrow: “You must work in security”.

"I… do", replies the man. "How did you know?"

“Well,” the robbery victim goes, “everything you told me is technically correct, but you’re not offering me any solutions or useful information”.

The man in the chair leans back, takes a sip of his beer, and grins: “You must work in management”.

"Excuse me, Sir, do you know what happened?"

The man in the chair replies: “Yeah, sure! Your house was robbed while you were away. It probably happened because you hadn’t locked your door, and the burglar alarm never rang”.

The man who’s just been robbed looks at him, raising an eyebrow: “You must work in security”.

"I… do", replies the man. "How did you know?"

“Well,” the robbery victim goes, “everything you told me is technically correct, but you’re not offering me any solutions or useful information”.

The man in the chair leans back, takes a sip of his beer, and grins: “You must work in management”.

After reading this article, you will:

• Know why practice and knowledge can not be replaced by technology alone
• Understand that we need knowledge to truly understand and solve problems
• Understand that theoretical plans are worthless without a practiced team

As of late, I’ve been pondering the idea that perfect security is unattainable. Some say there is no such thing as security, while others claim that there are only varying degrees of uncertainty. The notion that whatever you’re doing does not provide any real security is an uncomfortable thought. On the other hand, I’m sure most professionals agree that the idea of perfect security is naive at best.

If we elaborate, perhaps we can agree that most companies are struggling with varying degrees of (in)security. How we manage risk depends on a variety of factors: Our overall preparedness, level of training, appetite, luck, and so forth. Security does not have to be perfect in order to be beneficial. On the other hand, risks have to be manageable and/or acceptable. Some businesses understand this better than others. For example, credit card companies like Visa and MasterCard lose billions of dollars on fraud every year, but you are unlikely to see them going out of business anytime soon.

On the topic of managing risks, here’s a story that explains the situation many of my security colleagues face on a daily basis:

A man is driving his car on his way home from work. Pulling into to his driveway, he can immediately tell something is wrong. He steps out of the car and walks up to the front door, which is wide open. He peeks inside, only to see that his furniture is shattered and drawers have been ripped opened. The place looks like a mess. It’s obviously a burglary. Confused and afraid, the man walks outside. He stops on his lawn when he spots another man sitting in a reclining armchair on the other side of the street. Curious, he walks over and asks:

"Excuse me, Sir, do you know what happened?"

The man in the chair replies: “Yeah, sure! Your house was robbed while you were away. It probably happened because you hadn’t locked your door, and the burglar alarm never rang”.

The man who’s just been robbed looks at him, raising an eyebrow: “You must work in security”.

"I… do", replies the man. "How did you know?"

“Well,” the robbery victim goes, “everything you told me is technically correct, but you’re not offering me any solutions or useful information”.

The man in the chair leans back, takes a sip of his beer, and grins: “You must work in management”.

After reading this article, you will:

• Know why practice and knowledge can not be replaced by technology alone
• Understand that we need knowledge to truly understand and solve problems
• Understand that theoretical plans are worthless without a practiced team

As of late, I’ve been pondering the idea that perfect security is unattainable. Some say there is no such thing as security, while others claim that there are only varying degrees of uncertainty. The notion that whatever you’re doing does not provide any real security is an uncomfortable thought. On the other hand, I’m sure most professionals agree that the idea of perfect security is naive at best.

If we elaborate, perhaps we can agree that most companies are struggling with varying degrees of (in)security. How we manage risk depends on a variety of factors: Our overall preparedness, level of training, appetite, luck, and so forth. Security does not have to be perfect in order to be beneficial. On the other hand, risks have to be manageable and/or acceptable. Some businesses understand this better than others. For example, credit card companies like Visa and MasterCard lose billions of dollars on fraud every year, but you are unlikely to see them going out of business anytime soon.

On the topic of managing risks, here’s a story that explains the situation many of my security colleagues face on a daily basis:

A man is driving his car on his way home from work. Pulling into to his driveway, he can immediately tell something is wrong. He steps out of the car and walks up to the front door, which is wide open. He peeks inside, only to see that his furniture is shattered and drawers have been ripped opened. The place looks like a mess. It’s obviously a burglary. Confused and afraid, the man walks outside. He stops on his lawn when he spots another man sitting in a reclining armchair on the other side of the street. Curious, he walks over and asks:

"Excuse me, Sir, do you know what happened?"

The man in the chair replies: “Yeah, sure! Your house was robbed while you were away. It probably happened because you hadn’t locked your door, and the burglar alarm never rang”.

The man who’s just been robbed looks at him, raising an eyebrow: “You must work in security”.

"I… do", replies the man. "How did you know?"

“Well,” the robbery victim goes, “everything you told me is technically correct, but you’re not offering me any solutions or useful information”.

The man in the chair leans back, takes a sip of his beer, and grins: “You must work in management”.

After reading this article, you will:

• Know why practice and knowledge can not be replaced by technology alone
• Understand that we need knowledge to truly understand and solve problems
• Understand that theoretical plans are worthless without a practiced team

As of late, I’ve been pondering the idea that perfect security is unattainable. Some say there is no such thing as security, while others claim that there are only varying degrees of uncertainty. The notion that whatever you’re doing does not provide any real security is an uncomfortable thought. On the other hand, I’m sure most professionals agree that the idea of perfect security is naive at best.

If we elaborate, perhaps we can agree that most companies are struggling with varying degrees of (in)security. How we manage risk depends on a variety of factors: Our overall preparedness, level of training, appetite, luck, and so forth. Security does not have to be perfect in order to be beneficial. On the other hand, risks have to be manageable and/or acceptable. Some businesses understand this better than others. For example, credit card companies like Visa and MasterCard lose billions of dollars on fraud every year, but you are unlikely to see them going out of business anytime soon.

On the topic of managing risks, here’s a story that explains the situation many of my security colleagues face on a daily basis:

A man is driving his car on his way home from work. Pulling into to his driveway, he can immediately tell something is wrong. He steps out of the car and walks up to the front door, which is wide open. He peeks inside, only to see that his furniture is shattered and drawers have been ripped opened. The place looks like a mess. It’s obviously a burglary. Confused and afraid, the man walks outside. He stops on his lawn when he spots another man sitting in a reclining armchair on the other side of the street. Curious, he walks over and asks:

"Excuse me, Sir, do you know what happened?"

The man in the chair replies: “Yeah, sure! Your house was robbed while you were away. It probably happened because you hadn’t locked your door, and the burglar alarm never rang”.

The man who’s just been robbed looks at him, raising an eyebrow: “You must work in security”.

"I… do", replies the man. "How did you know?"

“Well,” the robbery victim goes, “everything you told me is technically correct, but you’re not offering me any solutions or useful information”.

The man in the chair leans back, takes a sip of his beer, and grins: “You must work in management”.
The robbery victim’s face glazes over with a confused look, and goes “I do. But, how did you know?”

The neighbor takes a long breath: “Well, you don’t seem to care why your house was robbed, but you expect me to be able to help. You are still in the same position as you were before we met, but now suddenly your house being robbed is somehow my fault”.

There are two points to this story:

The key message is that security professionals still have issues communicating with some of their more important stakeholders, namely those who give thumbs up and money to run day-to-day operations and new projects. Many in the security field don’t have the necessary know-how or experience to deal in terms of business risk, which makes communicating our concerns and ideas even more difficult.

Secondly, security professionals tend to put a lot of faith in technology. No one should ever think a door lock is so effective that you don’t need police protection, or laws that make it illegal for someone to break into your home. Security products will only solve part of our equation.

If we look at how “security” has evolved in the past 50 years, there have been some monumental changes. In the past, security was confined to the physical domain. By denying access to prevent harm or theft usually meant you stood a chance of succeeding. It sounds simple enough, but we are still trying to perfect how we do it. The good thing about physical risks and threats is that the human mind is hardwired to recognize them and act accordingly. Everyone knows what a robbery looks like, especially if someone points a gun in your face and asks you kindly to open up the vault.

In my opinion, the challenge is that we are now dealing with fundamentally different types of threats. Most of them are invisible. They are hard to grasp for individuals who do not deal with exploit techniques and software vulnerabilities on a daily basis. To make matters worse, the threat landscape is changing at such a rapid pace that we are struggling to keep up.

For all intents and purposes, even cyber security professionals are facing some serious challenges. Although we have been familiar with threats from malware and hackers for a long time, it is only recently we have been able to verify what some of our more advanced adversaries are capable of doing. Perhaps even more disconcerting, many companies simply have not allocated adequate resources to deal with cyber security in a responsible manner.

Why do I say this? Because most of the companies that have fallen victims to big breaches recently had the latest and greatest security technologies in place. Yet at the same time, it’s only recently that some of them hired their first CISOs, (usually after the breach, but that’s a topic for another time). Furthermore, most of their “security” teams often consist of old-school physical security staff who have had to learn a new trade, or people who initially started in a traditional IT-role, be it operations or development. This isn’t necessarily a problem. My concern, however, is that many businesses have placed too much faith in technology alone to solve their problems.

Some argue that there is a cyber security skills shortage, particularly in terms of finding the right person for the job. I would argue that many organizations simply are not spending enough time training and testing the people in charge of defending their crown jewels.

In June, I spoke at a conference where roughly thirty IT security managers form a variety of Norwegian businesses were present. I was on a first name basis with many in the crowd, and I knew that only one had actually provided relevant hands-on incident response training for his team in the past year. We all talk the talk, but only a select few really train for the inevitable. Moving forward, I believe developing your staff can prove more effective than relying solely on “solutions”.

When security teams introduce new defensive mechanisms and products into their environments, they are looking for increased automation, preferably something along the lines of “fire and forget”. However, without proper configuration and testing, many of these products only add “noise” when what you were looking for was actually better “signals”. The thing about paying for these solutions is that it partly removes the incentive to invest in knowledge of the problem they were supposed to solve in the first place!

On the other hand, for many companies, buying products and services makes perfect sense. Security might not be their “core business”, or at least they don’t think it is. In other cases, it may not be financially feasible. Regardless, the underlying issue is that product X might be too slow to adapt to new threats. Once upon a time, introducing firewalls and anti-malware products to your environment significantly increased your level of security. For many businesses, it made financial sense to invest in these technologies, both in terms of security, as well as reducing operational costs. They scaled better in the short term than manpower alone.

Nevertheless, I believe many organizations are walking a dangerous path by blindly relying on technology to solve problems they do not truly understand. In my opinion, we need to reinvest in knowledge in order to move forward.
The question then becomes: how do we move forward?

This winter, I attended a dinner with CISOs and CSOs from a variety of different companies. One of the dinner guests was Craig Rosen, who is the CSO of FireEye. During the dinner, Craig asked an intriguing question: “What does Nirvana look like for you, in your day job?” For Craig, the answer was simple: he wants the ability to go from detection to remediation in 10 minutes. For the majority of businesses I’m familiar with, this is a tall order. I do, however, think it’s an important idea. I believe defenders likely will work better against tangible goals against which they can measure their performance. They can adapt. I kept playing with this idea for some time after the dinner party, and came to the conclusion that stressing detection and response is key. If we look at Forrester’s hierarchy of targeted attack defensive needs – a model resembling Maslow’s hierarchy of needs – we can see that the ability to detect and respond to security incidents is at the zenith:

![Figure: The Targeted-Attack Hierarchy Of Needs](image)

Source: Forrester Research, Inc.

Unfortunately, detection and response is not a silver bullet. Aiming for the top without covering the fundamentals will not work. For more mature companies, however, the peak is key: if you are unable to catch the exploit phase and contain it within a reasonable period of time, you will lose. Data from thousands of breaches analyzed in Verizon’s 2014 Data Breach Investigations Report suggests that a motivated attacker will have successfully compromised your environment within 24-48 hours of having established their first foothold.

This leaves you with two options:

1. Choose to do nothing about it, because it requires hard work and prioritization
2. Face the challenge and solve it by investing in people, processes and technologies

Adequate detection and response capabilities will help you restore faith in whatever systems can still be trusted following a breach. Getting to this point, however, requires certain skills, mindsets, and perhaps most important of all: practice.

WHY PRACTICE?

In this day and age, it is not a question of “if”, but rather a question of “when” your organization will suffer the consequences of a breach. The data suggesting it likely already has happened to you is readily available. You might be breached right now and not know about it. For security managers, this implies that you will be looked to for leadership and guidance once the breach is eventually discovered. How do you handle this? Some might choose not to worry, because “they have a plan”. Plans are nice, but if we paraphrase the great warrior-poet Mike Tyson:

> “Everyone has a plan until they get punched in the mouth”.

If this makes sense to you, think about how you can empower your businesses to do the right thing. I encourage you to talk to your defenders, your responders, your engineers, anyone who will be vital to your response plan, and ask them what they need to succeed. Give them the necessary resources, and continuously test them to see if they make the cut. Time is your most valuable resource. Spend it wisely.
Predicting the future is always difficult, and the further ahead in time one tries to predict, the more challenging it is. At the same time it is important to have an idea of the longer time frame in order to be able to adjust our defensive abilities, be they in the form of personnel, tactics or modus operandi. There are few cyber defense players that are able to adjust their capabilities for the threats we will face in 2016. A relevant horizon to look towards in order to be able to alter capabilities is in the 4 to 8 year perspective.

As for the short term, I would say that 2016 will follow ongoing trends as we see them today. We will see slightly fewer cyber-attacks but with more severe consequences. The profit-margins of cybercriminals will continue to increase with relatively few risks involved. Nation states will continue to invest heavily in cyber capabilities, both of the offensive and defensive types, and cyber espionage will continue to be a significant challenge for businesses and nation states.

It seems to be a trend that opponents at the top-end of the threat scale, those with significant resources, use cyber-means as part of a larger campaign. This requires cyber defense to be seen in a bigger picture, and more closely coordinated with other security-areas in order to ensure a holistic perspective on security.

I further suspect more professional players are likely to see the value and benefit to be gained from using cyber means to alter information and situational awareness in order to achieve greater and more long-lasting effects from their operations.

Hopefully 2016 will be a year where we fully acknowledge, as individuals and organizations, that there are significant challenges facing us, challenges that we need to address by focusing on investing in security, rather than accessibility of digital services.

There are many challenges surrounding information sharing. Commercial considerations, security legislation and varying interests between different parties will always make sharing a challenge. Having said that much can be achieved through establishing arenas where the different players on the cyber field can get together in a spirit of trust and exchange knowledge and ideas in non-committing fora. Multi-departmental training- and exercise arenas are also a good opportunity to gain and share experiences, knowledge and information. As NATO, cyber defense players in general should change their principal mindset from ‘need to know’ to ‘responsibility to share’.

On the one hand awareness and the understanding of the risks affiliated with cyber challenges is increasing. At the same time one has to acknowledge that there are enormous values involved in this field. This means that our opponents are able to invest significant resources into continuously developing their attack vectors and offensive capabilities.

There is also a significant number of unknown unknowns. Zero day vulnerabilities are one example. We do not know how many of them are out there, we do not know how many our opponents are in possession of nor what they are able to do with them.

Until we know the full extension of the unknowns it is hard to answer the question, but were I to give an initial assessment I would say we are hard pressed to catch up to our opponents.
The Norwegian government is continuously developing its strategy on cybersecurity, and it released a revised action plan in September 2015. One of the strategic goals is to strengthen the cybersecurity knowledge and culture in the governmental sector. Whether you think that the human is the first or the last line of defence, it is beyond doubt that the human factor plays a key role in cybersecurity. In line with this, the Norwegian Centre for Cyber Security (NorSIS) is leading a project that aims to create a national metric for cybersecurity culture, which in turn will provide a more solid comprehension of how the Norwegian population relates to the inevitable digitalisation of their society.

The time for creating a national cybersecurity culture metric is long overdue. Yet, creating a metric is a challenging task. In this article, we examine the difficulties in measuring culture and present an approach to creating a national cybersecurity culture metric.

For a nation, a deeper understanding about a cybersecurity culture is of utmost importance as it touches upon some of the most profound questions for development. Not only does digitalization help businesses make smart use of information technology and data, it ensures citizens benefit from the digital age and it underpins economic growth. A safe e-citizen is fundamental to the success of the national digitalization. Mistrust in digital services and fear of online crime are some of the challenges that people face in the digitalization processes. Thus, we must understand the dynamics in how a cybersecurity culture is shaped and how it affects the digitalization in businesses, sectors and on a national level.

THE CHALLENGES OF MEASURING CULTURE

The main challenge in measuring cybersecurity culture is the concept itself. The emergence of the concept, as well as the day-to-day application of it, has made it problematic to utilize both vertically, amongst different types of business sectors, as well as horizontally, i.e. between different layers of society. The reason is simple: “Cybersecurity culture” is a concept first and foremost developed and applied within a business sector that is spearheaded by cybersecurity professionals and thus have cybersecurity as a primary focus. Thus, cybersecurity culture is a concept that has emerged within a rather limited and specialised cluster of industries, an industry with a sophisticated knowledge of cybersecurity parallelled by a keen interest in pushing the industry further. To put it simple: “Cybersecurity culture” is a concept developed amongst businesses that know what cybersecurity is. This does not hold true for a series of other types of industries, let alone for the Norwegian nation.
In creating a metric for measuring the national cybersecurity culture, there are at least two critical challenges: One is the question of terminology, i.e. what do we actually mean when we refer to “cybersecurity culture”? The other is that of level of analysis, i.e. how can we identify a “cybersecurity culture” concept that is valid and applicable to both businesses and nations? That is to say that whilst the concept might be developed within the confines of industries and businesses focused on cybersecurity, also nations have “cybersecurity cultures”. It may, however, not play out the same way. There is a huge gap in how “culture” is shaped and expressed depending on the level on which it is discussed. For example, whereas a business, an organisation and an institution all have defined purposes and thereby measures, the scope of a nation is much vaguer. Furthermore, while business can actively tutor and educate their personnel in cybersecurity, citizens of a state cannot be equally monitored. Is it, then, possible to generate a general comprehension of “cybersecurity culture” that is equally applicable to business and nations?

The term cybersecurity culture is not a new one, and there is no shortage in efforts to measure it. Although there doesn’t seem to be a clear and common understanding of the term, it is used to describe "something related to behavior". In other words: Cybersecurity culture is generally associated with the actions of employees. These are simple things to measure, so that is what the majority of cybersecurity culture metrics are set up to do. Different people grasp onto different aspects of cybersecurity behavior. They measure and extrapolate their findings.

But: Does this really say much about a national cybersecurity culture? Is the percentage of the employees that click on a phishing-link a useful indicator of cybersecurity awareness, or could it be just as much about the skill of the attacker? More importantly, these studies fail to explain how awareness is developed, how our personal values shape what we think about cybersecurity specifically and technology in general, or what role our interests plays in how we relate to cybersecurity.

**CYBERSECURITY CULTURE AS A TOOL**

Cybersecurity culture is a concept increasingly acquiring awareness. Be it cyber professionals or businesses and industries specializing in cybersecurity; all agree on the fact that the numerous technical advances in information sciences do not always produce more secure environments. Human factors influence how individuals interact with cybersecurity technology and it is this interaction that is often detrimental to security. Therefore, it is evident that solely technical solutions are unlikely to prevent security breaches.

Organisations have long since realised that the internal culture has critical impact on the organisation’s performance. It is the culture of the organization which extracts the best out of each team member. The culture develops a habit in the individuals which makes them successful at the workplace. Yet, given the degree to which businesses have acknowledge the impact of culture to its performance, it is interesting to notice how immature the discussions on cybersecurity culture are. The fact that cybersecurity actually have a cultural dimension should not come as a surprise to anyone. However, judging from the discussions on cybersecurity culture, one could easily think that it is. Cybersecurity culture is overall approached in two, yet intertwined, ways: Firstly, cybersecurity culture is considered as a tool in performance management. Secondly, cybersecurity culture is viewed as a sum of actions, a way the staff behaves. Cybersecurity culture, then, appears generally to be considered as behaviour patterns that can be altered and improved in order to increase the value added to a business or organisation. An obvious token of this approach is that cybersecurity culture tends to be discussed in terms of it being either “good” or “bad”. This normative over-tone clearly indicates how culture in the cybersecurity context is an aspect of utility, indicating that cybersecurity culture can be tested, measured and improved. This approach does, however, leave us with the obvious question: Is culture reducible to actions? And, is cybersecurity culture merely a tool for performance management and business governance? If so, it is tempting to ask whether the term “culture” may be imprecise. In no other context can culture be reduced to merely a set of actions.

In the social and cultural sciences, the term “culture” is considered far more complex and is rarely approached or described normatively. Rather, cultures are approached by scholars through a focus of the underlying ideas, values and attitudes that shape actions. Cultures are not tools; they place us in the world and shape our worldviews. In other words, actions and behavioural patterns are the expressions of attitudes and values.

**TOWARDS A HOLISTIC APPROACH TO CYBERSECURITY CULTURE**

There appears to be a clash of scholarly disciplines in the comprehension of “cybersecurity culture”. This does not come out of the blue: Cybersecurity and cultural studies have thus far been rather separated scholarly disciplines. The scientists dealing with culture have very rarely dealt with cybersecurity – and technologically scholar professionals have left culture to be studied by others. The reason is obvious. If you are an expert in cultural or social sciences, you do not have the skills to comprehend – or even engage in – the specialised language of engineers and cyber professionals. Yet, we believe that the analysis of cybersecurity culture benefits from a more comprehensive approach, wherein the competencies of cyberprofessionals and cultural scientists are integrated.

We believe that measurements of cybersecurity cultures can benefit from a more comprehensive approach, taking a step back from simple registrations of whether employees open phishing-emails and rather look at the attitudes towards technology and cybersecurity, and how this resonates with other core values, interests and abilities.

This project place itself in the middle of the discussion on how technology will develop our society further. You can also contribute to this, by becoming a partner to the project. Contact NorSiS to discuss how we can include your company or sector in our surveys.

For additional information, contact:

bjarte@norsis.no

Phone: +47 990 94 838

www.norsis.no
Faceing uncertainty is something cyber security professionals deal with on a regular basis. How vulnerable are you, really? What is the likelihood of a successful attack? Perhaps you are breached right now and don’t even know about it?

Facing uncertainty is something cyber security professionals deal with on a regular basis. How vulnerable are you, really? What is the likelihood of a successful attack? Perhaps you are breached right now and don’t even know about it?

Unfortunately, the risks posed by both known and unknown factors (e.g. uncertainties) are often hard to quantify. On one hand, one could argue that many of today’s cyber security challenges are solvable. On the other hand, the overall cost may be too steep. In terms of risk management, we can split uncertainties into “known unknowns”, and “unknown unknowns”. Known unknowns refer to risks we are aware of, such as outdated versions of software known for easily exploitable vulnerabilities. Unknown unknowns are trickier: These are the types of risks we have a hard time imagining. For example, they might not yet have resulted in observable damage or disruption. The human mind often falls short in this category because we tend to focus on risks with which we are familiar. For example, typewriter manufacturer Smith-Corona once sold tens of millions of machines yearly. However, they did not properly anticipate nor address the risks to their business posed by the advent of the personal computer.

At this point, you’re probably wondering what typewriters have to do with cyber security. While the example deals with competition from another industry, the point remains the same: as technology progresses, new risks will arise. Some of them may be lingering in the shadow, beneath our consciousness. As part of our annual practice, we aim to empower our customers by shedding
The goal of this article is to look beyond what is happening right now. By elaborating on the future and what it may have in store for us, we hope to provide the necessary foresight to ensure you stay ahead of the curve. The proverbial crystal ball that follows is structured into the following chapters:

- Moving from a “peacetime” to a “wartime” mindset
- Executives take the lead
- Governments vs. the people
- Cyber legislation as a global movement
- The industrialization of extortion

Unfortunately, our overall prediction with regard to cyber security is eerily similar to that one we offered in 2015: things are likely to get far worse before they get any better. With that being said, let’s begin:

MOVING FROM A “PEACETIME” TO A “WARTIME” MINDSET

Governments and businesses worldwide are gradually acknowledging the warning signs and alarms. The implications of the cyber security challenges we are facing are immense. Governments and businesses alike are gradually becoming aware of the potential consequences. Thus, we assess there will be a shift from “peacetime passivity” to a “wartime mentality”.

The risks posed by the inherent vulnerabilities in the networks that run our society are simply too great to ignore. As the Norwegian Government-appointed Committee on Digital Vulnerabilities eloquently pointed out, the radical social changes ushered in by decades of digitalization have revolutionized the way we work and communicate. At the same time, society has become dependent on a long line of complex and vulnerable value chains. While digitalization has revolutionized both how we live and work, many of the services we take for granted are vulnerable on a number of levels. Society has to change the way in which it addresses these vulnerabilities to ensure both consumer and commercial trust. An unexpected outage or debilitating attack on one part of the networks that run our society can have unforeseen, perhaps even catastrophic consequences. We are all stakeholders, but it will ultimately be up to governments and businesses to address these challenges, as consumers alone cannot individually decide how security is prioritized.

We believe the traditional emphasis on “checkbox” security compliance is nearly obsolete. Governments and businesses alike will need to properly understand the threats relevant to one’s environment in order to efficiently address them. This shift requires an intelligence driven model for cyber security. Without knowing one’s adversaries, most security measures will be nothing more than a shot in the dark.

EXECUTIVES TAKE THE LEAD


If you followed the news in 2015, you’ve already deduced the common denominator for all the before mentioned organizations. If not, the answer is that all of them fell victim to massive breaches. The list is by no means exclusive. If we had wanted to, it could have been much, much longer.

In terms of high-profile breaches, 2015 was not significantly different from the years before. A key difference, however, is that the organizations that so far have avoided the front pages are increasingly addressing cyber security both at the Executive and Board levels. Traditionally, cyber security risks have largely been the domain of the IT department. Now, businesses are maturing by addressing cyber security as an enterprise risk management issue. Security executives (e.g. CISO’s and alike) are increasingly called upon to answer the Board of Directors, who are rightfully concerned about their legal liabilities and responsibilities to their shareholders.

The potential impact on shareholders is key to the equation. Albeit an older story, the US energy technology company previously known as American Semiconductor Corporation (now named AMSC) experienced how shareholder relations can be affected by a breach first hand. In 2011, the company accused Sinovel, a Chinese competitor, of stealing intellectual property in the form of proprietary software used to control wind turbines. By 2013, Sinovel and two of its senior managers had been indicted by a grand jury in the United States for allegedly having used the stolen software in turbines installed in three Massachusetts communities. The incident, which by the end of 2015 consisted of no less than four separate legal battles against their Chinese competitor, has significantly affected AMSC’s valuation. At the beginning of 2011, AMSC traded at close to USD 300 per share, a price that by the end of 2015 had shrunk to roughly USD 6 per share. Naturally, the alleged intellectual property theft is merely a single factor. However, any company that loses their competitive edge – through criminal action or otherwise – will suffer at the hands of stock traders and investors.

In conclusion, our assessment is that Executives and Board Members alike will increasingly demand clear answers on how intellectual property and trade secrets are secured, how their cyber security strategy aligns with business goals, and whether their organization is capable of detecting and responding to breaches.
GOVERNMENTS VS. THE PEOPLE

In the early 1990s, the US government began removing export restrictions on technologies related to cryptography. These very restrictions had enabled the United States Intelligence Community to eavesdrop on the sensitive communications of both their allies and their enemies for decades. The ability to implement cryptographically secure communications arguably changed the world in ways we have yet to fully grasp. However, some argue that secure communications represent a trade-off: the very same technologies that protect political activists, whistleblowers and privacy-concerned citizens are also freely available to those with less honorable intentions.

In the past few years, several easy-to-use technologies have empowered virtually anyone to communicate securely with minimal risk of eavesdropping. This development has sparked a new debate over the use of strong cryptography. Several oppressive regimes are flat-out denying their opponents access to such tools. Perhaps more disconcerting, Western democratically elected governments are seeking the ability to place government-mandated backdoors in cryptographic communication services and software, arguing that the threat of terrorism outweighs the people’s need for privacy.

The United States and Great Britain have arguably been the biggest proponents for placing government backdoors in encrypted communication technologies. Fortunately, the US administration recently reversed its decision to pursue these backdoors following harsh criticism from both academia and industry professionals. The final blow was given in the summer of 2015, when a joint team of scientists and cryptographers published a report named “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications” – recommended reading for any interested in the subject. The Norwegian Government-appointed Committee of Digital Vulnerabilities in Society (Lysneutvalget) echoed the report in their final report, recommending Norwegian authorities to oppose initiatives seeking to regulate or ban encryption, and urging them to fight any such efforts on an international level.

mnemonic supports the Committee’s recommendation. However, though this battle may be won, the war is far from over. There are still numerous challenges ahead in terms of both covert and lawful surveillance and interception. Towards the end of December 2015, the head of the Norwegian Intelligence Service told the Norwegian politicians that he wanted access and control over all digital communications traversing in and out of the nation. Anyone familiar with network security monitoring can appreciate the need for better visibility and data retention. On the other hand, critics argue that blanket surveillance may undermine our democratic society as we know it. If citizens are aware they are being monitored, it is fair to assume that some may change their behavior. Perhaps they will refrain looking up certain types of information, or in effect censoring themselves by avoiding dialogue altogether. We do not have the answers, but the questions stemming from the proposal are worthy of a national debate.

Thus far, the average citizen has been more than willing to trade privacy for convenience. Both mobile applications and cloud services enjoy unprecedented access to the data we rely on to organize our lives. The very same data is of great value to governments – oppressive or otherwise – who have incentives to monitor their citizens. Our assessment is that (democratic) governments likely will seize the opportunity to access our data unless citizens refuse. Demanding oversight and governance around data ownership, secure services, culpability for breaches, and the right to privacy will be paramount in this fight. The people need to draw a line in the sand by asking: what kind of society do we want to live in?

CYBER SECURITY LEGISLATION AS A GLOBAL MOVEMENT

At the end of November 2015, the European Union Parliament enacted the EU Network Information Security (NIS) Directive. The directive, which will be implemented into law by the EU member states, members of the European Economic Area (EEA), as well as “operators of essential services” (e.g. critical infrastructure) by 2017, will fundamentally impact the way security policies are shaped and breaches are reported. In addition to the NIS Directive, other initiatives are seeking to unify the existing EU data protection regulations into a single law.

Once formally adopted, individual member states will have until the end of 2017 to implement the Directive. When in place, the laws will require significant changes for a broad range of companies. One of the key requirements of the Directive is the mandatory reporting of incidents no less than 24 to 72 hours after the initial discovery of the breach. Organizations and businesses who are in the scope of the Directive will be required to report incidents that may impact the continuity of services (e.g. confidentiality, integrity or availability). These incidents may be publicly disclosed by the controlling national authority (e.g. a national Computer Emergency Response Team – CERT) in order to achieve the public awareness required to appropriately prevent further damage or contain the incident.

Failure to comply will result in financial penalties and other sanctions, depending on the scope and the type of incident. The exact figures for imposed penalties will vary depending on the scope and severity of the incident. However, the Directive states the penalties must be “effective, proportionate and dissuasive”.

Our assessment is that few Norwegian organizations are ready for the changes ahead. Our recommendation is that critical infrastructure operators in energy, healthcare, transportation and financial services should prepare to adopt the Directive. This includes:

- Reviewing internal security policies and mechanisms to ensure they comply with audit requirements set by the relevant national authority
- Building and testing a cyber security incident response program that will comply with the reporting standards (e.g. notifying a national CERT 24 – 72 hours after the initial discovery)
- Implementing advanced cyber security mechanisms to detect and prevent attacks, as the Directive mandates businesses to implement “state-of-the-art” security mechanisms that “guarantee a level of security appropriate to the risk”.

...
• Establishing dedicated roles for overseeing cyber security and incident response programs, coordinating with the Board of Directors, Executives, and General Counsel.

As the Directive is to be fully implemented by 2017, businesses are likely to face significant challenges unless they prioritize these actions in 2016.

Despite the challenges ahead, we believe the NIS Directive is a step in the right direction. The legal obligations and reporting requirements will likely give a wide variety of organizations and businesses the incentives needed to address security concerns on a wider scale than what we are currently observing. Assuming the EU and EEA member states implement the Directive in similar fashion, the harmonized enforcement of the laws will likely ensure increased security across a multitude of value chains. In the end, this is positive for the consumer. However, legislation alone only solves part of the puzzle. Without strong national authorities to enforce compliance and provide coordinated response options, we may see a sector-based fragmentation in terms of security posture. Considering that virtually all sectors are interconnected, having a clear “weakest link” may be a valuable target for those who wish to do us harm.

THE INDUSTRIALIZATION OF EXTORTION

Cybercrime has taken many shapes in the past few years. In previous years, we have seen increasing sophistication, moving from simple Trojans, to fake antivirus software, to exploit kits. In 2015, extortion has positioned itself as a center of gravity for financially motivated cyber criminals. Ransomware using strong cryptography hit new heights in the past year, and our assessment is that this is only the beginning. As the value of stolen credit cards is decreasing, criminals are seeking new ways to secure their incomes. Consumers who have had their credit cards stolen are often blissfully unaware until their bank calls to inform that they are shipping them a new one. Monetizing information involves a multitude of challenges. Ransomware is different. It’s personal. Criminals control your data, and you have to sort out the mess yourself. Compared to many organizations, your average consumer often does not have similar backup mechanisms to ensure a speedy recovery.

Extorting money from users have proven to be lucrative line of work. By forcing victims to pay in anonymous and nearly untraceable crypto currencies such as Bitcoin, criminals are allowed to operate with impunity. The use of strong cryptography has forced countless victims to pay up, as there is simply no feasible way to recover encrypted files. Based on reporting from several sources, victims who pay the ransom get the decryption key in return. This should come as no surprise. It’s in the criminals interest to hold up their end of the deal. Should word get out that paying the ransom is useless, victims will refrain from doing so. Thus far, these extortion tactics have primarily targeted files present on the victim’s computer, as well as resources they have access to (e.g. network shares and removable drives).

Moving forward, we expect an increase in these types of attacks against other platforms. The attack on Ashley Madison is likely a noteworthy precursor of what is in store for 2016 and beyond. Some data never expires. Healthcare records, browsing habits, what was said and done on certain websites are typically information users do not want exposed. One can recover from losing access to personal documents and photos. On the other hand, information regarding adultery, disease, unethical behavior and the like have the potential to destroy lives. Victims of this type of extortion will be pushed to their limits, and will likely be willing to pay far more to ensure their records never see the light of day. Using extortion to attack your reputation may very well be the next big thing, and we expect the ransoms to become far higher.
We have seen an explosive growth in cybercrime during the last decade. Potential rewards for cybercriminals are far greater than those from traditional physical crimes, and the risk is much lower. To capture these rewards, criminals have become more sophisticated with technology and their social engineering methods, and they continue to develop new tools and tactics to achieve their goals. In this report, we will investigate the trends in cybercrime threats against online banking.

ONLINE BANKING – A GAME OF CAT AND MOUSE
A significant challenge in the world of online banking is providing a secure service that is accessed from assumed insecure devices – namely customers’ personal computers. This approach has resulted in an arms race between criminals and banks.

In such an arms race, the ability to anticipate or predict new attack trends is a great advantage for the defender. Thus, our goal will be to analyse past trends, identify their causes, and use that knowledge to predict and manage future trends.

While the main focus is online banking, the recommendations are applicable to other types of cybercrime as well.

PAST TRENDS
One of the first attacks against online banking was e-mail phishing of user names and passwords. Criminals would then later use these credentials to steal money from a customer’s account.

Once banks deployed two-factor authentication with time limited one time codes (OTCs), this simple phishing tactic became ineffective. The criminals responded by developing real time phishing attacks, where they would use the credentials immediately after they were obtained.

Banks responded by requiring customers to first use an OTC to log on, and then use a second OTC to confirm payments. The criminals responded by phishing multiple OTCs. One tactic involved presenting a forged log on page to the customer, then after the customer provided the OTC to log on, an error message was displayed saying “An error has occurred, please wait five minutes and try again.” With the first OTC in hand, the criminals could then log on to the customer’s account, prepare
a fraudulent payment, and capture the second OTC required to confirm the payment when the customer tried to log in a second time after waiting 5 minutes.

When banks deployed SMS as a channel to distribute OTCs, criminals responded with mobile malware that could intercept and forward SMS messages.

When banks deployed payment verification using secure hardware tokens, where the customer confirmed the payment contents on a separate, secure device, the criminals responded with more sophisticated social engineering techniques used to trick the customer into confirming a fraudulent payment.

Some banks deployed hardware and browser fingerprinting to differentiate legitimate banking users from potential fraud attempts. The criminals responded with malware that allowed remote control of the customer’s own computer, and used that computer to commit the fraud.

The response from some banks was also deploying systems for click path analysis to attempt to distinguish real human behavior from automated tools used by criminals. The criminals responded with automated attacks designed to emulate human behavior, including random delays.

And so the game of cat and mouse goes on.
CAUSE AND EFFECT
The trends from criminals have one thing in common: they are reactions to new security controls deployed by the banks. Thus, the cause of these trends is that banks deploy new security controls to stop current threats.

There may be other external causes as well, such as law enforcement actions or new cash out opportunities, but most of the trends in threats against online banking are reactions to new security controls.

Having established the cause, we can try to predict future trends by examining recent advancements in security controls.

PREDICTION
Behavioral biometrics, or keystroke dynamics, is a security control that is being applied to online banking. The principle behind keystroke dynamics is to analyze how a customer enters information in addition to the information content. A system can be trained to recognize a customer and their keystroke behavior, and issue an alert if it is likely that someone other than the legitimate customer entered the information.

If this security control becomes prevalent and prevents current attacks, then the criminals will adapt. The most likely response is that when phishing credentials, they will also record how the credentials were entered, and replay the precise sequence of events to the online bank to mimic the customer’s exact keystroke behavior. Such an attack can easily be implemented either in malware on the customer’s computer or in JavaScript on a phishing site.

THREAT MANAGEMENT
Having established the cause and effect of cybercrime threats, we can now investigate how to manage these threats. We have seen that criminals respond with new tools and tactics to defeat new security controls.

To gain the upper hand, a bank should figure out how to break a new security control before it is deployed. Once they have broken the new control, they should determine how to detect the attack that breaks the control.

This approach implies that a combination of visible (prevention) and invisible (detection) controls are used. One example of a visible control is two-factor authentication, while an invisible control could be an intrusion detection system (IDS).

The bank should also carefully consider how to respond to alerts from the invisible controls. In order to protect the detection mechanisms, it is important not to leak any information to the attacker. If an attacker is able to detect an invisible control, then that control becomes visible to the attacker, who will then try to break it. For example if an invisible control returns a verbose error message, the attacker can modify their tactics and evaluate their success in how the error message changes or disappears.

RECOMMENDATIONS
1. It all starts with people
Our most important recommendation for successfully fighting cybercrime is having the right people. Whether these capabilities are achieved internally, through security partners or the security community as a whole, the fight against cybercrime requires security professionals whom dedicate their time to information gathering, analysis and detection, even in quiet periods.

We recommended breaking new visible security controls before they are deployed, which requires experienced security professionals to both break the control, and find a method to detect the attack. The threat landscape changes frequently and a defender has to adapt. There are no “silver bullet” products that are able to do this without experienced people.

2. Detection and response tactics
Our next recommendation is to develop detection mechanisms and response tactics, and maintain them as a process. Part of this process may include:

• Obtain timely and relevant threat intelligence, gather all relevant data, and correlate and analyse data in near real time to detect attacks.
• Develop signatures for known threats and anomaly detection for unknown threats.
• Predict attacks against new security controls and ensure that the detection mechanisms are able to detect the attacks.
• Use response tactics that do not leak information to the attacker.

3. Threat information needs to be shared
Finally, we strongly recommend sharing threat information. Share threat information with other banks and security organisations to reduce the criminals’ rewards. Share threat information with law enforcement to increase the criminals’ risks.

There are many areas of business to compete in, but uniting to fight cybercrime should not be one of them.
What threats do you see on the horizon for 2016?

We expect to see more targeted attacks (also used for crime/theft, not just espionage), and more social-engineering based attacks.

How do we achieve more sharing around incidents?

We are working on this; there are no simple answers. Basically need to sell the “need to share” idea.

For us, we’re increasing the non-public sharing between our members – this is working well. We’re also recommending that they share incident information publicly whenever that makes sense – which happens regularly, particularly when customer services are involved.

We are also participating in closed national and international sharing groups/networks.

Are we gaining or losing terrain?

Overall in society we are not gaining yet, but I hope we’ve slowed down the loss.

In the financial sector I believe the banks are holding their terrain reasonably well.
INTRODUCTION

BEAST, CRIME, #gotofail, Heartbleed, Freak, Breach, Poodle, Logjam.

Use RC4. Don’t use RC4. Use AES. Don’t use AES-CBC. Don’t use SHA-1. Use RSA. Don’t use RSA, use ephemeral Diffie-Hellman. Use elliptic curves. Or not. Don’t use SHA-1. Use 128 bit keys, or at least 112 bit keys. Don’t use 1024 bits, use 2048 bits. SSL. TLS. WTF!

With a steady stream of vulnerabilities, an unreasonable amount of acronyms, and ever-changing expert advice, it has been nigh impossible to keep track of the current “best practices” for SSL/TLS over the last few years. In this article, we take a shot at clearing up some of the confusion.

SSL VERSUS TLS

Secure Sockets Layer (SSL) was the protocol invented by Netscape in the 1990s to enable e-commerce. Transport Layer Security (TLS) is the successor protocol, building on SSL v3.0, and was standardised by IETF in 1999. While the name SSL has stuck in many people’s minds, today it is a dead protocol. The POODLE attack in 2014 was the final nail in the coffin, and use of SSL is completely deprecated.

TLS itself exists in three versions, 1.0, 1.1, and 1.2. For many years, TLS 1.0 has been the dominant protocol version. This has largely been due to inertia, with TLS 1.0 being “good enough”, and no clear incentive to change. Over the past few years, the inadequacies of TLS 1.0 have been exposed, and on the web, TLS 1.2 is now well supported by modern servers and browsers. As a step towards better communications security, it will in many cases be necessary to move away from TLS 1.0.

For instance, version 3.1 of the PCI-DSS industry standard expressly forbids the use of TLS 1.0 as a security mechanism after June 30th 2016. Migrating to a newer version of TLS will thus be an imperative for applications that handle cardholder data. For web-facing applications this may be reasonably easy, as support for TLS 1.2 has become widespread. However, it is very likely that many legacy systems on the backend and for business-to-business communications have not been updated to support newer TLS versions out of the box. For these systems, there may be a lot of work to be done in the first half of 2016.

After reading this article, you will:

• Get a better understanding of the world’s most widely used crypto protocol
• Clarify some of the common misconceptions surrounding TLS
• Look at some of the developments being adopted at present, and arriving in 2016
SECURITY PROPERTIES

TLS as a protocol aims to offer point-to-point security. That is to say, properly configured, TLS 1.2 will provide confidentiality, authenticity and integrity for a data connection between two communicating hosts. To do this, TLS builds on several underlying cryptographic algorithms, such as the Advanced Encryption Standard (AES). In many cases, the choice of algorithms is not mandated by the protocol, but part of the configuration. There are many cipher suites to pick from, and not all of them are secure.

Over the last few years, vulnerabilities have been found in all aspects of TLS: the protocol itself (specified across multiple RFCs), the underlying algorithms (notably MD5, SHA-1 and RC4), and different protocol implementations (such as Heartbleed in OpenSSL, or #gotofail in Apple’s Secure Transport library). In fact, every common TLS stack had at least one critical vulnerability in 2014. The combination of widespread use, a complex technical protocol, and a high level of scrutiny all but guarantees that further vulnerabilities will be found.

Since TLS is a point-to-point protocol, it does not offer end-to-end security along a communications chain with multiple hops. A very common pattern is to use TLS to protect data on public networks (such as the Internet), but terminate TLS at the enterprise boundary, and transmit data in the clear internally. Common arguments against this is that it is hard to set up, that it inhibits debugging and IDS/IPS functionality, that certificate management is difficult, and that performance suffers.

While the performance argument appears dubious in practice, the other arguments are relevant. However, transmitting sensitive information, whether passwords, personally identifiable information, confidential documents or payment card information in cleartext on internal networks is often not an acceptable risk, even if it has been tolerated in the past. Blanket use of TLS, also internally, is likely to be a significantly simpler approach to protect network communications than myriads of application-layer crypto plumbing such as WS-Security.

TLS AND PERFORMANCE

Performance-wise, the heavy lifting in TLS comes with session establishment. Performing a TLS handshake to establish a secure channel for the first time requires using public-key crypto algorithms, such as RSA or Diffie-Hellman, which are CPU intensive. Furthermore, moving to larger public key lengths to increase security gives a marked increase in CPU cost: as a rule of thumb, doubling the key size of RSA (e.g. from 1024 to 2048 bits) brings an 8-fold increase in the computational cost.

Fortunately, the cost of transmitting data over a live TLS connection is much less. When using TLS with a fast cipher, such as AES or ChaCha20, it is generally not a problem to transmit data at line speed with a marginal CPU cost close to zero. Furthermore, TLS sessions can be paused and resumed very efficiently with minimal overhead.

Thus, there is a very large difference between the performance requirements of a TLS service handling a large number of ad-hoc sessions with a large number of different end-users (e.g. the front-end cluster handling https://www.example.com/), and a TLS service communicating with a few, stable clients (e.g. a database server handling TLS connections from a fixed set of application servers). The former is likely to be doing a large number of TLS handshakes with new clients, and needs CPU and/or dedicated hardware support to match. The latter can use long-lived TLS sessions with resumption, with new handshakes few and far between, and an amortized cost close to zero.

CONTENT INSPECTION

Use of encrypted network communication makes life harder for anyone wanting to listen to the traffic – that is, after all, the entire point. Unfortunately, this also makes life harder for legitimate inspection, particularly in a corporate setting. Whether for debugging purposes, or security functions such as data-loss protection, intrusion detection / prevention systems, or use of a web security proxy, persistent encryption makes life harder for the defending side as well.

For web traffic as well as some applications, use of public key pinning and mandatory use of TLS, as well as the “perfect forward secrecy” ciphers, makes interception even harder because it is no longer possible to use a proxy to decrypt traffic. The same features that Google are rolling out to prevent rogue regimes from eavesdropping on Gmail users makes it just as difficult to perform legitimate inspection of traffic between a corporate endpoint and those same Google servers.

While tapping network communications and decrypting TLS on the side is a viable approach in some cases, it is increasingly necessary to gather the data where it is actually available in an unencrypted state in order to get at the data. Increasingly, this means gathering data from system log sources, and possibly also using endpoint management tools in more invasive ways than before.

SECURE CONFIGURATION PROFILES

A widespread problem with rolling out TLS across an organization is inconsistent configuration. It stems from the (very real) perception that TLS can be difficult to configure, that it is configured differently depending on the implementation used, and that there are a large number of individual configuration points. As a consequence, TLS settings are chosen on an ad-hoc basis, leading to widely inconsistent security profiles.

The only reliable approach to solve this is standardization. Define secure TLS configuration profiles for all widely-used platforms, maintain these as part of central configuration management, review and update the profiles regularly, and enforce them as a standard throughout the organization. Since TLS is a network protocol, verifying that TLS-protected network services are consistent with the standard is fairly easy to do with a scanning tool.

\[1\] As the infamous “TLS added and removed here! :/” slide from the Snowden leaks demonstrates, this approach has clear weaknesses.

Original article: “NSA infiltrates links to Yahoo, Google data centers worldwide. Snowden documents say.”

The IETF TLS Working Group is currently standardizing a new TLS version 1.3, which addresses many of the protocol shortcomings that have been discovered over the last few years. As with all design-by-committee, this process is taking some time, but we expect that TLS 1.3 will be finalized in 2016.

At present, it appears that TLS 1.3 will improve on TLS 1.2 and previous versions on most fronts, both simplifying the protocol while improving performance and security. As with all new standards, it is an open question on how long it will take before stable TLS 1.3 support is widespread in server and client software. However, the momentum behind TLS development now is much greater than when TLS 1.2 was released in 2008.

Meanwhile, there are several other interesting developments, mainly driven by the web security use-case. While not a mandatory feature of HTTP/2, use of TLS is much more closely integrated in the new HTTP specification. Security headers such as HTTP Strict Transport Security (HSTS) and HTTP Public Key Pinning (HPKP) can be utilized to instruct browsers to use HTTPS and certificates in more restricted ways. Use of perfect forward secrecy (PFS) crypto mechanisms has already become quite common and usage will continue to grow. In 2016, we will see more use of TLS and more secure use of TLS.
When mnemonic reports a security breach

97.03%

of the time it is correct. This is way above the average in the business.

2015 had an

11.2%

increase in reported security breaches from 2014
When an organization makes a strategic decision, there are always associated risks to take into account. Put simply – we want to know what can prevent us from succeeding. A goal of information risk management is to reduce the uncertainty about our chances of success. When we know the risks we face, we can mitigate or accept them.

The business value of information risk management is twofold. Firstly, it helps organizations make strategic choices knowing the risks they are accepting, and make plans to manage the risks. Secondly, it helps us establish a security strategy that associates specific security costs with the organizational strategies they are designed to protect. This allows us to identify the return on security investment (ROSI). It also ensures cost effective security by only protecting assets at the level required by their importance.

INFORMATION RISK MANAGEMENT

I use the term “information risk management” (IRM) rather than just “risk management”. This is because I want to emphasize that we are concerned about all information; digital, verbal or in documents. We are also concerned about processes and routines as well as applications and systems.

In a complex organization, there will be risks at different levels. There will be high-level risks that affect the organization as a whole (financial risk, reputational risk, legal risk, etc.), and operational risks that can contribute to a high-level risk (denial of service, hacking, industrial espionage, etc.). These risks can have complicated relationships; a risk in one area can increase the risk in several other areas.

Weaknesses (vulnerabilities) in the systems, processes and applications that process, store and transport critical information can affect each operational risk. One vulnerability can affect several operational risks. It is this complexity that IRM is designed to address.

IRM AS A FRAMEWORK

The implementation of an IRM framework works best as a project. This allows the progress to be monitored accurately, and to identify problems early so they can be handled quickly.
At mnemonic, we have divided the IRM framework into five sets of activities:

1. Identify

A critical first step in implementing an IRM framework is identifying the goals and values of the organization. By understanding the environment in which it operates, it is then possible to identify the risks in that environment - the risk profile. Establishing the risk profile ranges from identifying the threat agents to understanding the constraints under which the organization operates: laws, contractual requirements, internal standards and policies. Workshops with senior management are an effective method for information discovery and building the organization’s risk profile.

2. Classify

The information gathered from the Identify activity is used to define acceptable levels of risk - the risk appetite. Types of information are identified and classified in terms of the potential consequences for the organization should it be leaked, corrupted or unavailable when needed. Ranking these consequences against the risk appetite, we can identify critical information.

With the information types and their respective importance classified, it is straightforward to apply the same classification level to the processes, systems and applications that process, store and transport the information. The most critical systems process the most critical information. The required level of security for these systems is based on how critical the information is. This is our security baseline.

At mnemonic we perform the Classify activities in several ways. We identify the broad groups of information with management to focus on priority areas. Working with the information and system owners within the focus areas, we develop classification tables and finally define the required security levels.

3. Assess

The organizational risk profile is used to identify operational risks that could contribute to one or more organizational risks. We know what level of security we need, but what level do we actually have, and how well is it working? This is where risk assessments come in.

Risk assessments examine the critical processes, applications and systems and identify any weaknesses that could cause operational incidents. These weaknesses could be administrative, technical, process related, amongst others. Subject matter experts in several areas must be included in the assessment to ensure all angles are covered.

With potential weaknesses identified, there may also be a requirement to test whether there are controls (passwords, locks, routines, etc.) in place, that make it less likely that it could cause an operational incident.

Through this process we can begin to estimate the level of risk connected with each process, system and application.

4. Treat

The Treat activity addresses the vulnerabilities that are not fully controlled, or are too severe to accept. There are a many controls that can reduce risks; procedural, administrative, or technical monitoring and analysis of network traffic to name a few. Some risk treatment is straightforward and can be implemented locally. We should co-ordinate treatments that involve several areas through a risk strategy. A risk strategy identifies cost effective, managed approaches to security.

The ISO 27002 standard lists a large number of control types that can be used to mitigate risks. The standard however doesn’t cover all areas and should be used as a reference rather than an absolute rule. Care should also be taken when implementing controls in isolation - it is more effective and likely cost efficient to introduce controls at a high level that cover many underlying weaknesses.

5. Monitor and Report

Risk management is a cyclical process rather than a one-time activity. The efforts and true value of a risk assessment are lost if the findings are not followed up or used to provide an overall risk landscape that management can use to support their strategic decision-making.

A risk register is utilized to record and track identified operational risks, vulnerabilities and their respective treatment plans. Risk owners monitor the treatment plans to ensure they are completed, with the effect on identified risks reassessed regularly. The assignment of a Risk Manager (one or several) aids in this process.

Choosing a risk assessment approach

Standards generally describe what activities are part of risk assessment, but not specifically how to do the activities. The framework and methods appropriate for your organization will not only differ from other organizations, but they will likely change and evolve over time. mnemonic’s risk assessment methodology is based on internationally recognized standards and methodologies, and continues to evolve based on experience and information risk developments.

Below is a short list of useful references as a starting point:

- ISO/IEC 27001, 27002, 27005 and 31000
- NIST Cybersecurity Framework
- Lockheed Martin Kill Chain Analysis
- NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- CIS Controls for Effective Cyber Defense – v6.0
A Risk Manager will have the responsibility for coordinating risk reporting, ensuring consistent risk assessments, and lifting risks’ ownership to the level necessary to ensure they are properly addressed. The results of all risk activities are used to improve the process for next time, resulting in continuous improvement.

A Corporate Risk Manager may be desirable for larger organizations, with responsibility for identifying how operational risks can affect organizational risks, and aggregating the results for management.

And of course it is essential to update the risk profile, risk appetite and threat intelligence whenever major changes occur, either internal or external.

**SUPPORTING IRM WITH TECHNOLOGY**

For large or complex companies, a GRC system (Governance, Risk and Compliance) that automates many of the activities in IRM is well worth the investment. A GRC system can reduce the impact of IRM on the employees, avoid the need to employ more people and automate collecting and reporting on control activities. GRC systems also provide a dashboard to visualize risk information, appropriate for each level of management, and allow drill down functions to gain detailed information.

**CONCLUSION**

This may seem a daunting project to take on and indeed, it makes demands on any organization in terms of attention and resources. Plan activities over at least one to two years to allow new processes and procedures to be accepted and become part of the normal daily work. Start simple and build slowly. Make sure that results are made visible to everyone, put information on the internal network about the number of risk assessments carried out, the number of potential risks that have been mitigated and so on. And don’t forget to recognize the efforts people are making, and to celebrate your success.
What threats do you see on the horizon for 2016?

An increased number of advanced attacks on services, as well as multi-channel social engineering to achieve the threat actors target. Unfortunately, I think identity theft will become more common. In most cases and in the end of the day the goal of the attackers will be financial gain.

How do we achieve more sharing around incidents?

Being open concerning security incidents is important. Security industry and the media have an extra responsibility in this matter.

Are we gaining or losing terrain?

There is a high level of awareness around security in all parts of the value chain, producers to consumers, so I hope we are gaining terrain.
VULNERABLE TO VULNERABILITIES – HOW DO WE KEEP UP?

Written by: Espen Martinsen, Senior Consultant

After reading this article, you will:

- Know the differences between traditional vulnerability assessments and CVM (Continuous Vulnerability Monitoring), and establishing vulnerability situational awareness

Vulnerabilities are a natural byproduct of software development. Software is only as secure as its weakest link, and with the constant wildcard that is the human element, combined with increasing complexity and rapid development, software will inherently have vulnerabilities.

Modern security regimes accept and expect that vulnerabilities will be encountered and place an emphasis on managing vulnerabilities before they can be exploited.

TRADITIONAL VULNERABILITY ASSESSMENTS

In the world of IT security, a vulnerability assessment can be defined as an activity to identify, evaluate and prioritize weaknesses in software. From a historical perspective, a vulnerability assessment has comprised of the following activities:

1. Initial demand for an assessment (either planned or due to a discovered threat)
2. Contact made with appropriate party to deliver vulnerability assessment (internal or external)
3. Contract and/or relevant paperwork
4. Agreement about scope
5. Actual testing, scanning, removing false positives and assessment
6. Report writing
7. Presentation to explain report and findings
8. Changes approved and established
9. Re-test done
10. Presentation of report after re-test

Generally these steps take anywhere between 3 weeks and 3 months, though it can take even longer in select cases.

So how does this process measure up against today’s rate of vulnerability discovery?
THE VULNERABILITIES JUST DON’T STOP

Vulnerabilities in publicly available software, open source or commercial, are registered and tracked through the global CVE (Common Vulnerabilities and Exposures) system. While this system does not track vulnerabilities in publicly available services (e.g. a net bank), it does provide an indication on the trends of vulnerability discovery.

New CVE records per year:

So what does this table tell us?

In 2003, there were approximately four vulnerabilities discovered daily. By 2014, this number has exploded to 26 vulnerabilities a day. To look at it another way, by 2014 it only took two months to discover more vulnerabilities than were discovered in all of 2003. The trend for 2015 looks much the same as 2014.

This table shows that despite advances in security technology and secure coding awareness, there is an upward trend in the number of vulnerabilities discovered each year.

What does this table not tell us?

CVE’s represent vulnerabilities in publicly available software, and it is this software that is used as the foundation for not just millions of websites, but also the critical infrastructure controlling energy production, water distribution, financial systems and pretty much every digital service we have come to rely on as a society.

That means that each of these vulnerabilities represents an exponential impact in the real world. For example, the Heartbleed vulnerability (CVE-2014-0160) was estimated to affect approximately 500 million devices globally, including 17% of all secure web servers using certificates from trusted authorities and 50 million Android devices.

Nor does this table tell us the length of time between software being published to when a vulnerability is disclosed. Shellshock (CVE-2014-6271) was discovered in September 2014, however it has been determined the vulnerability has existed in the Unix Bash shell since September 1989. While it took 25 years to discover the vulnerability, and the CVE was published with a fix, successful attacks were discovered only one hour after the vulnerability was disclosed and in less than a week more than 1.5 million Shellshock-related attacks were being recorded daily.

So even if you’re performing a vulnerability assessment of your exposed services bi-annually, almost 5000 new vulnerabilities will have been discovered between each assessment. And just as security practitioners have vested interest in new vulnerability publications, so too do the attackers.

So what can you do to narrow the gap between when a vulnerability is disclosed and knowing if you’re affected?
CONTINUOUS VULNERABILITY MONITORING (CVM)

Continuous Vulnerability Monitoring (CVM) is a concept which has gained momentum over the past couple years, popularized by NIST SP 800-137. The principle of CVM is to perform regular, automated security scans to gain a continuous understanding of the vulnerability status in an environment.

Similar to anti-virus products that have a virus definition database updated daily (or hourly), the security scanner is consistently updated with recently published vulnerabilities. This way, those managing vulnerabilities in an organization will receive updated information regarding:

• New vulnerabilities found
• Closed vulnerabilities (fixed)
• Changes in findings
• New hosts appearing on the network
• Missing or dead hosts on the network

While the frequency of the scan will vary to support an organization’s requirements, it is quite realistic to perform scans daily reporting on the delta with full summary reports issued on a monthly basis.

Excerpt from NIST SP 800-137:

“Information security continuous* monitoring (ISCM) is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.”

*The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed, analyzed and reported at a frequency sufficient to support risk-based security decisions as needed to adequately protect organization information. Data collection, no matter how frequent, is performed at discrete intervals.

With a CVM initiative, the end result is a level of situational awareness of the risks within their systems that is up to date on a daily basis rather than bi-annually, or even longer.

SOUNDS GREAT! SO WHAT’S MISSING?

The automated reports generated by security scans will generally be accurate, but also quite technical. This leaves interpretation, understanding, prioritization and internal presentation in the hands of those receiving the reports within the organization. Perhaps most importantly, the results require context to understand the consequences the vulnerabilities may pose to the business.

These are the values that are added by having an experienced professional reviewing, interpreting, validating, and contextualizing the scanning results. In our experience, it is the written report and presentation of the findings rather than the technical scanning results that convey the necessary messages of the scan (see: consequences) to both management and system owners.

ARGUS CONTINUOUS VULNERABILITY MONITORING – TAKE IT A STEP FURTHER

mnemonic’s Argus Continuous Vulnerability Monitoring service adds additional layers to CVM. By incorporating vulnerability scan results into an Argus Managed Defence service, SOC Security Analysts will have increased context when analyzing security incidents, make more informed decisions and ultimately reduce the impact to the business.

If a server is exposed to an exploit attempt and from CVM we can confirm the server is vulnerable to the attack, the criticality of the response, and thereby the response process can be adapted to reflect the increased risk. Likewise if CVM helps to confirm the server is not vulnerable, resources will not be unnecessarily wasted because of a false-alarm.
It is difficult to predict future threats, as both technology and expertise level is changing continuously and rapidly. However it’s still possible to make some predictions about the future.

In my opinion, mainly, the following topics will be the most important challenges we will have in 2016:

• The polarization in the political arena in the international community is going to affect activities in the cyber world too. As a result of this we’re going to see more and more sophisticated attacks against critical infrastructure between rival countries.

• Mobile devices and their applications will create new challenges for us, security people. Mobile devices are going to become more and more relevant as the gateway for malicious activities against large enterprises.

• I suppose, systems which process big data are going to be an attractive target for various type of malicious actors in the near future.

Of course it is important to follow the evolution of cyber threats and keep yourself up to date with predictions about future threats, but ultimately we need to focus on what is really relevant to our business.

At any given time, we must have a clear picture of what we have to protect and how to protect these. In this context it is of course important to mention a good contingency plan which must be updated and well implemented in the organization as well.

Transparency. The industry needs to move towards an attitude where being attacked is not considered as a weakness. Sharing information is key, and as of right now the industry is lacking a hub for information sharing. An independent organization for coordination of activities against cybercrime and for information sharing can help us in our fight against cyber criminals.

We win battles, but the war will never end. Based on our response to attacks, the attackers develop new methods – and so on. The increased attention towards cyber security in society is a good tendency, and makes us better equipped to respond to attacks.
APPLICATION SECURITY IN A SELF-SERVICE WORLD

After reading this article, you will:

• Look into key security differences between traditional IT and self-service web applications
• Learn about structured approaches to combine software security with modern application development practices

INTRODUCTION

In the old days, the world seemed to be simpler. Perimeter security still seemed sufficient. External (untrusted) actors did not, at least not by design, interact with internal (trusted) systems. While information exchange across organizational boundaries did occur, it was largely point-to-point between trusted partners. Thick client applications communicating over some proprietary format were not uncommon.

In these days, security was largely based on static mechanisms, like IP addresses and passwords, and often founded on general obscurity. Software development tended to long cycle lengths, with few and large go-live events due to waterfall-style development projects and sluggish change-management processes. Security testing was an activity that could be carried out by an external contractor every year or so.

However, this is no longer the case. Agile methodologies, cloud platforms, open web standards and self-service IT all bring significant benefits to the table, with shorter time to market, simpler maintenance and lower operational costs. At the same time, the borders of the enterprise are becoming increasingly porous.

Commonly, the main goal of an IT project is to expose a defined set of functionalities, including those functionalities that used to be strictly internal, to users from the Internet at large. In this setting, security must become an integral part of how one designs the interaction with the IT systems, as well as the software development lifecycle itself. While perimeter security is still necessary, it is no longer sufficient to mitigate the inherent risks in an interconnected, self-service world.

In this article, we will take a brief look at some complementary approaches to application security that may be useful in adapting to this situation.

THE RISK LANDSCAPE

From a business perspective, exposing internal data and functionality to the world often makes a lot of sense. At the same time, there are plenty of risks that need to be managed. Even minor mistakes and disruptions quickly become very visible, and may have a disproportionate impact on the reputation of the company and service in question.
For instance, “Kenneth (36)” became a minor celebrity in Norway in 2012 when his name and address was exposed to a few thousand users of the government portal Altinn, owing to a latent and unknown bug in a load balancer. Even though the actual damage must be considered minor, with no sensitive data leaked (contrary to initial media reports), and no sensitive business functionality exposed, the reputational (and political) damage to Altinn was severe.

Meanwhile, opening the perimeter to expose internal content to the world at large also means that a threat agent wanting to penetrate the enterprise has two new avenues of attack at their disposal; either aiming for weaknesses in the application infrastructure, or attacking through the application itself.

Many of the largest data breaches over the last few years have been accomplished through attacks on the application layer, typically either by SQL injection or by achieving remote code execution. In this article the focus is on the application layer risks.

SELF-SERVICE SECURITY ARCHITECTURE

A useful perspective to help understand the security needs of a self-service application is to look at the abstract security capabilities needed to support the functional security requirements. As an example, for an operational self-service web application, the following capabilities are likely to be necessary:

1. Cryptography: The ability to use cryptographic mechanisms to provide confidentiality and integrity services where appropriate, for instance through use of Transport Layer Security (TLS) to protect sensitive data in transit over the Internet.

2. Authentication: The ability to uniquely associate end users with local identities – whether through use of a local user store, or through federation with a centralized or external identity provider.

3. Authorization: The ability to make access decisions based on relevant context information, encompassing both static parameters such as user identity and roles, and dynamic parameters such as the specific functionality and data being accessed.

4. Content inspection: The ability to make security decisions based on application layer data, identifying malicious activity in an application context, taking appropriate actions, and raising alarms. For instance, use of a Web Application Firewall (WAF) or an XML gateway to protect against malicious requests.

5. Flow control: The ability to restrict network communication flows so that they follow defined communication patterns and rules; for instance, to prevent users from bypassing security infrastructure and accessing back-end systems directly.

6. Mapping: The ability to translate between different security models, security domains, and security contexts in a structured way, maintaining traceability along the way. For instance, translating user identities from external to internal representations, mapping HTTP session cookies to internal security tokens, and handling delegation for users acting “on behalf of” another party.

7. Logging and analysis: The ability to gather relevant security information, as well as other context, correlate it across multiple systems, provide alerts, visibility and analytics, and retain appropriate audit information.

These capabilities are chosen to support an operational IT system that is servicing customers and providing value by supporting business processes. Other security capabilities will be applicable to different settings, for example to support specific needs during software development, or an information security management system (ISMS).

It can be an illuminating exercise to look at an existing application infrastructure, and consider how these security functionalities map to the existing architecture, whether they are all there (and relevant), and whether there are additional security capabilities that need to be present.
SECURE SOFTWARE DEVELOPMENT FRAMEWORKS

Adopting a standard framework for secure development is a useful way to structure security-related activities for organizations that develop software. One of the leading frameworks in this area is the BSIMM (Building Security In Maturity Model), which is an open (Creative Commons-licensed) framework that provides a library of 112 useful security activities presented in a structured manner.

One of the most appealing aspects of the BSIMM framework is that it is based on real-world data from the software security programs at 78 different companies from a variety of industries and sectors. This means that the activities are tried and tested, and also that it is possible to compare notes.

BSIMM provides both horizontal comparisons between the different companies in the latest version of the study, but also longitudinal data for the companies that have participated in several BSIMM versions. It can also be used to create a scorecard for one’s own organization.

Another important aspect of BSIMM is that the activities aren’t narrowly focused on software development, but views the development lifecycle as one of four domains. The other three are Governance, Intelligence, and Deployment. By doing this, BSIMM paints a very complete picture of activities that can be used to support a software security initiative.

I highly recommend looking at BSIMM as a catalogue of activities that are out there – much as ISO 27002 is often used as a catalogue of “useful and common security controls”. While it is perhaps unrealistic and not practical to implement BSIMM from cover to cover, it provides practical guidance with respect to activities that at least should be considered as part of a software security initiative.

AGILE SECURITY AND AUTOMATION

In an agile development setting, a major goal is to reduce time to market by pushing new functionality to production quickly and iterating. While regular external security assessments and penetration tests are still a necessary part of an application security program, periodic assessments every three or six months or ahead of major changes are likely to be insufficient. This because there can be few large changes but many minor ones that may introduce flaws. The potential window of exposure may simply be too long if a vulnerability is inadvertently introduced.

To do agile security well, it is necessary to integrate the security activities much more closely with the everyday agile process than compared to processes with longer cycle times. Development teams need to have security champions present who can ensure that the relevant questions are being asked through the entire process – from backlog grooming and design, during construction, in peer reviews and during testing. Misuse-cases should be defined, and backlog items with a high security impact should be identified early to make unwanted scenarios visible.

On the technical side, the scope of test automation should be increased to cover automated source code analysis, security testing and fuzzing, as well as catching security-related regressions. A major challenge here is to ensure that the false positive rate (“noise”) is not too high, while still gaining useful results. Heavy non-deterministic tests, such as dynamic vulnerability scanning and fuzzing, should probably not be integrated with the “main” continuous integration pipeline, but may still be run in parallel. Deploying to production frequently (or even continuously) also means that one must be able to either roll-back or deploy a patch rapidly if a critical issue is discovered in the live environment.

CONCLUSION

As Fred Brooks wrote in 1986, there is “no silver bullet” to kill the complexities present in large-scale software development. Security is no exception to this rule. Breaking open application silos and moving to short development cycles and frequent releases makes security more difficult, and an increased investment in software security may be a necessary cost to achieve those gains.

While these challenges cannot be avoided entirely, having a structured approach to software security does help ease the pain. So does building the skills and security knowledge of all involved parties. To succeed, security must be an integrated part of software development, rather than an afterthought.
Client side attacks
– effectiveness of malicious code

Attacks against internet facing services
Industrial Ethernet is emerging as the dominant technology in distributed control systems and converging the whole communication network - from the office to the field level. Within the Nordic region, we see the same emerging trend in new deployments across industrial sectors, including process, power and marine.

In line with this, the industry has been moving towards Commercial Off-the-Shelf (COTS) solutions to fulfil networking functions, which has opened the pathway for direct interconnection between company administrative networks and the automation systems. While this has facilitated easier data exchange, it has also opened the possibility to attack the previously isolated automation systems from or through the company network.

INDUSTRIAL SECURITY LANDSCAPE

Industrial deployments were traditionally built as isolated islands, thus security was more a question of doors and walls than IT. Employees from the operations department had the responsibility to keep the communication network intact.

Threat analyses show that industrial systems can also be more prone to Denial of Service (DoS) and related attacks due to the stricter Quality of Service (QoS) requirements and lack of available processing power in the devices. The result is a network infrastructure that can handle a magnitude higher traffic than the end-node.

While engineering efforts have been made to reduce the risks associated with interconnectivity, security has only really gained momentum in industrial environments after the more recent incidents like STUXNET and repeated cases of DoS incidents coming from external networks.

SECURITY IS NOT ONE-SIZE-FITS-ALL

A natural progression for securing Ethernet based industrial environments is adopting security solutions used in more mature Ethernet networks - namely the everyday office network. A challenge with adopting office security solutions for industrial networks is these solutions are being re-purposed: they are designed to operate in a different environment and fulfil a different set of requirements.

Amongst others, the QoS requirements of an automation system tend to drastically differ from
those of an office network, and carry potentially life-threatening consequences should QoS fluctuate. In an office network, poor QoS may merely result in a VoIP call being dropped, whereas in an automation system the consequences affect the physical world and can be far more devastating.

**BRINGING SDN INTO THE MIX**

Besides the efforts on adopting IT security solutions to industrial environments, several working groups are involved in introducing security solutions into automation protocols and protocols used to support an automation system (e.g. IEEE 1588v3 on security functions, IEC 61850 to have integrity protection). The necessity of network management systems are gaining acceptance to support life-cycle management of the communication infrastructure.

In this landscape, SDN is a promising technology to support automation vendors to deploy their distributed control systems (DCS) more effectively. This will allow easier brownfield extensions and to have a detailed overview of the traffic under operation.

The central control of communication allows separating traffic and control. This enables deployment of new services without disturbing the production network, and the appealing possibility of having a full overview of network flows from one central controller. These are all useful features in an industrial context as they allow continuous monitoring of QoS and better separation in case of shared infrastructure.

Using several planes in a communication technology is not a novelty; it was present in Asynchronous Transfer Mode (ATM), and Synchronous Digital Hierarchy (SDH) or all the digital cellular networks. What is new is that these management possibilities are now available also in a much smaller scale. The forwarding performance is expected to be very similar or equivalent to the current non-SDN switches used in Ethernet networks (flow control causes some signaling overhead).

**ADVANTAGES OF SDN**

The detailed flow control capabilities introduced with SDN allows testing and resource reservation (meeting QoS requirements) not just at commissioning, but also during operation. The ability to isolate new traffic flows can be beneficial from both security and operational viewpoints.

Decoupling forwarding from control also allows faster reaction on network disturbances, such as employing pre-calculated backup routes, which also assist in meeting QoS requirements.

As part of the universal use of Ethernet communication, it is now common for vendors to share the network infrastructure to operate different parts of an installation. With SDN, it is possible to create an overlay network that follows the logical topology of an application or subsystem. This would improve the control possibilities as the staff could follow the communication paths in a more natural way.
SDN AND SECURITY

With the SDN controller maintaining a complete view of the network flows, it is easier to implement an Intrusion Detection System (IDS) or to implement Managed Security Services (MSS).

Current IDS implementations typically use port mirroring or distributed wiretaps to create a copy of traffic for analysis. While possible to segregate traffic by VLAN and some other methods, monitoring points are commonly limited to the local interface.

SDN can take this functionality into a new level. The controller has a complete view of the Layer 2 traffic streams over the whole network, thus not only has a wiretap everywhere, but also has control of the forwarding entities. It can make changes in the forwarding decisions in real time, thus reaction on non-legitimate traffic can happen before the first frames reach the end nodes.

The successful operation of MSS is also supported by the typical traffic pattern on an automation network: the majority of sessions are machine to machine (M2M) and in QoS sensitive cases, typically periodic and predictable.

This overprovisioning also supports the SDN operation when new flows need to reach the controller prior to the forwarding decision. The static traffic pattern will also allow the use of sharp heuristics on new traffic, allowing a deny-all-like approach with isolating non-whitelisted traffic from existing legitimate traffic flows already in forwarding.

CHALLENGES WITH SDN

The first group of issues relate to the SDN controller. To allow a central entity to control and configure the whole network, it has to gain administrative access over the whole network infrastructure configuration and status. Thus, the SDN controller’s ability to control an entire network makes it a very high value target and a single point of failure. An SDN controller needs to be accessible by the switches in order to take forwarding decisions. It is a traffic management challenge to place the SDN controller in a way, where all the switches can access it and it is not crossing boundaries of different network zones. Alternatively, each network zone could get its own controller at the expense that each controller will only have a total overview of the zone it controls.

In addition, typical access control and logging features must be extended for SDN. Examples here include logging and supervision of configuration changes in the controller and to provide background information on forwarding decisions for forensics.

THE FUTURE

SDN is very likely to be the next big step in industrial networks. It offers exactly the functionality automation engineers are looking for: hiding the network and allowing the planning and deployment of network infrastructure without deep technical knowledge, based only on the definition of network flows and automatic dimensioning rules.

By allowing fine-grained traffic control, enforcing security through the SDN controller and enhancing logging capabilities, SDN will allow industrial networks to take a much needed leap forward in gaining security and operational excellence.
Ransomware attacks, particularly those incorporating encryption (Cryptoware), will remain a main threat, targeting anything that may provide an important service and/or store relevant data.

Due to a lack of security- and privacy by design combined with poor patch/vulnerability management, we expect to see the continued criminal use of existing, tried and tested exploits. But we also expect to see new generations of malware that will continue to target not only customers but also corporations directly, using more encryption and information hiding techniques. This will further complicate malware analysis and frustrate digital forensics. We also expect to see a rise in mobile malware, including mobile malware families that are going to be cross-platform.

In general, we expect an increase in the use of anonymization and encryption technologies by criminals to protect their identities, communications, data and payment methods. In the area of payment methods, we expect a wider adoption of cryptocurrencies such as Bitcoin by criminals.

As data will remain a key target and commodity for cybercriminals, we expect an increase in data breaches. This will be facilitated by the already mentioned lack of security- and privacy-by-design but also the increased attack surface created by the Internet of Things, trends such as BYOD and third-party dependencies.

The increasing adoption of the IoT will create additional attack vectors and a broader attack surface. It will also complicate patch/vulnerability management. A single fault in a software and/or hardware component will potentially affect a large number of devices.

We also expect a further shift to card-not-present fraud as some countries such as the US, traditionally a main cash-out destination for card-present fraud, is in the process of adopting EMV technology.

Moreover, malware attacks on ATMs will remain a key threat.

Growing Internet coverage in developing countries and the development of streaming solutions providing a high degree of anonymity (e.g. decentralized and built-in Bitcoin support), will likely further the trend in the commercial live streaming of child sexual abuse.
How do we achieve more sharing around incidents?

This requires creating effective and efficient trust relationships between the parties concerned. It also requires identifying the incentives for sharing and the development of a joint business case that specifies what will be shared, for what purpose, what will be done with the information, etc.

LE needs to build on its operational successes with a view to increasing confidence in its ability to investigate both effectively and discretely. For LE it is essential to build and develop working relationships with the private sector, the CERT community, and the financial sector including banks, money transfer agents, virtual currency scheme operators and exchangers. While this requires harmonized and effective legislation and regulations - and the transposition therefor - LE should also aim to stimulate the voluntary and proactive engagement of these partners.

Finally, effective sharing also requires standardization of data formats and terminology.

Are we gaining or losing terrain?

The 2015 IOCTA contains many examples for LE successes in the fight against cybercrime. This has been made possible by the increasing level of international cooperation between main cybercrime divisions within the EU and with those of non-EU partners, and the alignment of priorities throughout the EU. Another key aspect contributing to the success in the fight against cybercrime is the close involvement of private sector partners.

However, cybercrime is certainly increasing in terms of volume, number of attacks and economic damage. It is also evolving at a high pace. As a consequence, there is a constant need for LE to keep up with the latest developments, which requires regular training and education, the right tools and close cooperation with the private and the financial sector as well as academia. This all needs to be supported by adequate budgets. As some countries outside the EU are increasingly getting online, which will create opportunities for criminals to attack victims in these countries but also to use the infrastructure in these countries.