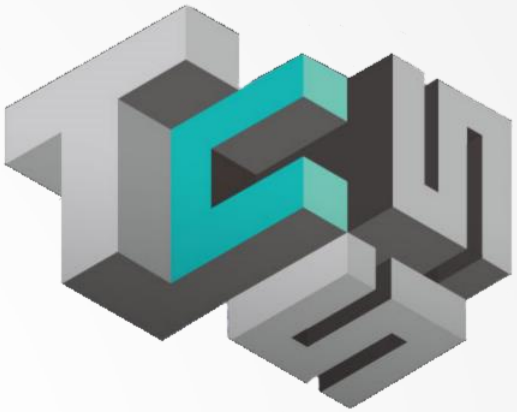


FINSEC Network Security Issues and Trends from 2016 (and Beyond)

Taiwan Cyber Security Summit 2017

Ian Farquhar

Gigamon Security Subject Matter Expert

Document version 1.0 Updated 14/MAR/2017 Status: RELEASE

Ian Farquhar

GIGAMON SUBJECT MATTER EXPERT FOR SECURITY

Gigamon - Subject Matter Expert for Security (Current)

RSA/EMC - Security Technology Evangelist

- Designated an EMC Thought Leader by EMC OCTO
- Designed the Security Architecture for Lockheed-Martin's successful Bid for the Australian Department of Defence "Central Processing" Tender
- R&D work with RSA OCTO on Hardware Security

Cisco – Network Security Consulting Engineer

- Network Security Consulting for customers including: Telstra (Australia), Malaysia Telekom, KLIA (Malaysia), China Construction Bank, Guangdong Development Bank (China), Shanghai Telecom and others

Sun Microsystems – Network Security Engineer

- Developed and maintained Sun's technical security standards
- Security representative on SunIT Governance Council
- Incident response, investigation and intelligence gathering

Silicon Graphics – Product Support Engineer

- AUSCERT contact for vulnerabilities in SGI products
- Member of the Worldwide vulnerability reporting team
- SGI liaison for the Supercomputer User Group
- Involved in the SGI "DESchall I" project

Macquarie University – Research Engineer

- Member of the CSIRO-funded team which did the initial engineering for the 802.11 (Wi-Fi) standard, responsible for R&D into L3 mobility (mobile-ip) and security evaluation

Education

- Macquarie University – Bachelor of Science (Computer Science and Electronics)
- Post-graduate study in Cyber-Defense strategies commencing in 2017, focusing on hardware and firmware implant detection and mitigation strategies

Public Presentations (partial list)

- IEEE MILCIS (2015)
- AUSCERT (2013, 2014)
- Singapore Governmentware (2013, 2014, 2015)
- Cisco Live! (2015)
- Monetary Authority of Singapore (2008)
- Tech Dimensions (2011)
- Cryptography and Architecture Committee member and panel moderator for the RSA Conference Beijing (2011)

Specific Areas of Expertise

- Network Security Architecture
- Security Operations
- Investigations and e-Forensics
- High-Assurance Security Hardware Implementation
- Reverse Engineering (performing and preventing)
- Block and stream cipher design, implementation and cryptanalysis
- Cryptographic Key Management
- Security Operations
- Security and Privacy Governance
- Data Loss Prevention Technologies
- SSL/TLS Interception
- Ultra High Speed Packet Processing for Security

Disclaimer

Predictions and other comments are offered only for general discussion purposes, and are not intended as guidance or recommendations for specific organizations and should not be viewed as guarantees.

Agenda

FOR MORE DETAILED DISCUSSION SEE MY CONFERENCE PAPER

- Threat landscape changes leading up to 2017
  - Hacktivism as a tool of non-hacktivist threat actors
  - Targeting of Financial Industry Infrastructure
  - Denial of Service and the Internet of (Insecurable) Things
- Issues and challenges in FINSEC
  - Strategic: The false dichotomy of “Prevent” vs. “Detect/Remediate”
  - Architectural: do we have network perimeters anymore?
  - OSI Layer 8 and 10 Attacks
- Ten predictions for the next ten years

Gigamon®

Threat Landscape Changes 2016

A Taxonomy of Threat Actors

WHO ARE OUR ADVERSARIES?

- Threat actors:
  - The usual “four horsemen of the cyber apocalypse”: nation state hackers, terrorists, hacktivists, and financially motivated criminals
  - Malicious insiders
  - Malicious/disreputable commercial organizations
  - Marketing, advertising and data brokers (local and foreign)
  - Journalists and investigators (limited domains)
  - “Ego” hackers and script kiddies
  - Others (“RAT voyeurs”, security researchers, the “make” community – typically limited domain)
- “Limited domain” means that these groups are threats in specialized areas
- Not all of these are directly relevant to financial orgs
- “Financially motivated criminals” includes crypto extortionists

Hacktivism as a tool of non-Hacktivists

BACKGROUND

- Hacktivism is relatively old (term coined in 1994 by Cult of the Dead Cow)
  - A portmanteau of “hacking activism”
- Traditional hacktivism was closely tied with traditional “activism”
- Recent high-profile examples where hacktivism seems to have been used by or involved non-hacktivism threat actors:
  - Sony Pictures Hack, 2014
  - US Democratic Party, 2016
- In all cases, the aim seems to have been overtly political, rather than a traditional “activism” approach
- While claims of attribution for both are made, conclusive proof remains elusive

Hacktivism as a tool of non-Hacktivists

RISK ASSESSMENT

- Could hacktivism be used against a financial institution?
  - Yes!
  - Arguably already has been, although the typical breach source was from an insider threat
- Countering this, the financial industry has a lot of experience with audits and oversight. Despite this, audits in financial investigations regularly find highly damaging personal correspondence, even between senior banking officers
  - Example: recent government investigations into banking practice in Australia
- FSI also often faces audit requirements which mandate the long-term storage of communications
- Hacktivism has been a major focus of security in government, and this attention needs to be replicated in the FSI industry also.

Hacktivism as a tool of non-Hacktivists

POTENTIAL SOLUTIONS

Technical Solutions

- Data Loss Prevention and similar Deep Content Inspection technologies can help
- Typical DLP tools were installed for compliance only, but have a valuable capability to detect other threats to the organization
- DLP developed a poor reputation between 2008 and 2011. It's time to revisit this technology, and for use-cases beyond compliance, especially for network DLP.

Policy and Governance

- Don't keep old data or communications around for no reason – archive it offline (or delete!)
  - Old data no longer needed has negative value: it is a potential threat vector!
- Set enforced archive policies on data stores, and enforce that policy
- Consider encrypted and non-persistent messaging technologies for mundane communications

Behavioral

- Educate staff on the possibility of data breaches – this is just acknowledging a possibility, not an admission of failure. Use media reports of data breaches at other organisations to reinforce this training
- Encourage them to evaluate any correspondence (email, instant message, anything with persistence) in terms of the consequences of it becoming public
- Where regulation requires the long-term archiving of communications, ensure that all staff recorded understand that this is happening

Targeting of Financial Industry Infrastructure

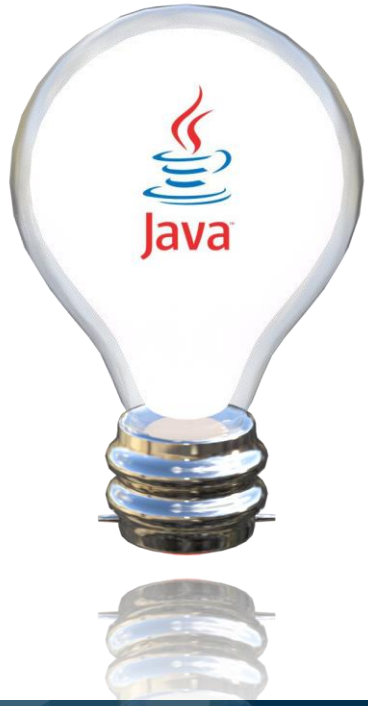
BACKGROUND

- The SWIFT attacks in 2016 were a wake up call to the FSI industry
- As an industry banking has moved or is moving to real-time transfers and settlements
- The original 24-48 hours banks had to notice and detect fraud is now fractions of a second
- Analytic analysis remains the best approach to detecting this fraud, but remember the tiny time window
  - Some money will be lost, but you can significant reduce impact
- The biggest challenge is the shortage of data scientists needed to create the model for high-speed fraud detection, and determining which data is valuable with sufficient signal to noise ratio

The Internet of Things (IoT)

LET'S TALK SCALE

- Term coined by British entrepreneur Kevin Ashton in 1999
- Originally popularized through the Auto-ID centre at MIT in 1999 during the dot.com bubble
- Scott McNealy: "putting Java into light bulbs" (2000)
- There is no agreed-upon formal definition yet
- A subset of the "Internet of Everything" – all Internet connected devices
- ABI Research says:
  - 10 billion wirelessly connected devices (2013)
  - Over 30 billion devices expected by 2020
- Devices per head of population:
  - 2013: 7 billion (1.43 devices per person)
  - 2020: 7.7 billion (3.90 devices per person)



Denial of Service

2016 WAS AN “INTERESTING” YEAR

- We are all familiar with Distributed Denial of Service attacks
- The top 5 DDoS attacks of 2016 (according to Tripwire):

	Target	Botnet Used?	Peak Bandwidth	Nodes in Botnet
1	Dyn	Mirai	n/a	100,000
2	Brian Krebs	Mirai	620Gbps	n/a
3	Clinton and Trump Campaign Sites	Mirai	n/a	n/a
4	Rio Olympics	LizardStresser	540Gbps	n/a
5	5 Russian Banks	Mirai (uncomfirmed)	n/a	24,000

- n/a = not available

IoT BOTNETS!

Source: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/5-significant-ddos-attacks-2016/

What Is Wrong With IoT Security?

THE ECONOMIC MODEL SUPPORTING SECURING IOT DEVICES IS BROKEN

- IoT products will be sourced from all tiers of the market: consumer to bespoke
- Priced from very low cost to extremely high cost
- The bulk of products will be in the consumer marketplace:
  - Bill of Materials optimized for cost
  - Engineered for large production runs
  - Built within a product cycle which may be measured in months
  - All will have compliance frameworks, but compliance is likely to be voluntary
  - Yet may be installed in places where:
    - It may run for decades
    - It will be forgotten unless it fails
    - The identity of the responsible individual may be unclear
    - There will be no maintenance (“are all your light-switch security patches up to date?”)

Current IoT Security Approaches

NOT ONE OF WHICH IS A TOTAL SOLUTION

- **Deny/ignore the problem**
  - Subset: “make the money and run”
- **Address it on a per-device basis (the predominant approach)**
  - Extremely expensive, doesn’t scale
- **Standards**
  - Assumes that security is a fixed state. Security isn’t.
  - Can also work against you (eg. Medical devices and the need to recertify any software change)
- **“Encryption”**
  - This is not really an approach, just a “make the problem go away” buzzword. It’s actually “deny/ignore” in disguise.
- **Platformization**
  - How did that work out for Android? I can still buy devices running Android 2.x!
  - It has worked for Apple, but how do we scale that beyond a single company?
- **Virtualization**
  - This is really just a multi-level security (MLS) architecture
  - Succeeds or fails on how many exceptions to the defined security model are needed to make the device function as designed
- **Containment**
  - “We’re not going to solve this at the endpoint. Let’s contain (quarantine) the device so it can’t do damage.”
  - Very much a “public health” approach to IoT security

IoT Security Issues Not Just DDoS

IOT DEVICES ARE ENDPOINTS

- The proliferation of insecure IoT devices plus widely available upstream network bandwidth is why IoT platforms make such good botnet hosts
- But the risk goes beyond DDoS:
  - IoT devices will be finding their way into your networks, officially or unofficially
  - IT may not know where these devices are
  - They may have security issues which will never be patched
  - Consider them as a viable platform to attack as a stepping stone into your org
  - Your network (especially wireless) design needs to accommodate the identification, segregation and control/monitoring of all IoT devices

Issues and Challenges for FINSEC

Strategic Approach to Threat Prevention

PREVENT VS. DETECT/RESPOND

- Many orgs proudly proclaim they're following a "prevent" strategy
- Others claim a "detect/remediate" strategy
- THIS IS A FALSE DICHOTOMY
- Both approaches are essential, as they complement each other
- Detect/Respond is needed because all risk determination techniques are approximations
  - Comment: detecting "badness" in a piece of unknown executable code is fundamentally a restatement of the Turing Halting Problem
  - Fact: unknown "bad" will get through, and detect/respond is essential to catching the actions of the malware or attacker
- Protect filters out the "known bad" so they don't overwhelm "detect"

Architectural Approach to Threat Prevention

WHERE OH WHERE DID MY PERIMETER GO?

- Banking networks are typically the most complex and varied of all
- The idea of security monitoring and control being completely at the network edge (whatever that is nowadays) is no longer viable
  - It really never was viable, we just pretended it was for a couple of decades
- At one extreme we have Google's BeyondCorp approach
  - All controls deployed at the endpoint
- At the other we have network microsegmentation, where all endpoints are isolated and communications are explicitly opened
  - Difficult to deploy and manage
  - Even today most FSI firewall teams face a challenge deploying restrictive traffic policies
  - Some security architects doubt the actual value of microsegmentation

Architectural Approach to Threat Prevention

SOME QUESTIONS

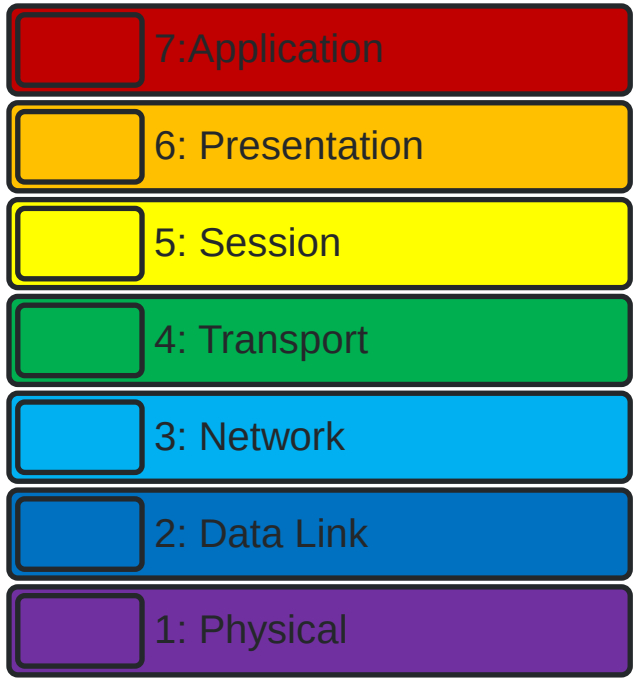
- Question: if I have no edge to my network, where do my “prevent” (blocking) tools go?
  - One of the reasons we put them at the edge was because they simply weren’t fast enough for core networks
  - Inline tools are now available which are capable of running at core network speeds
  - Inline tools need to move into the locations where they see the most traffic, including east-west traffic inside the organization
- Question: if I have boundaries everywhere (eg. Because of microsegmentation), how do I monitor it?
  - The efficacy of switch SPAN/mirror ports remains poor, and they’re limited
  - Host-based agents add to endpoint complexity, and can be a risk vector themselves
  - We need to engineer networks to support visibility of all traffic everywhere

Description, Characteristic, Decision Makers

Denial	Product	Compliance	Risk	Operational	Assurance
There is no focus: this customer does not believe there is a genuine security issue	Focus is on buying the right product (usually single product), and having it deployed. All problems go away.	Focus is on meeting a compliance, regulatory or legal requirement to the letter, usually in the most minimal and cheapest possible way. Security is conflated with meeting this compliance requirement.	Focus is on governance, risk and compliance. Security is seen as a risk management exercise, governed by the needs of the business.	Focus is on operational excellence. Security is seen as a lifecycle of architecting security, operational vigilance, and constant update of their capabilities.	Focus is on understanding that the claimed security properties of all components are reliable, have known (safe) failure modes, and are not red threaded (backdoored).
Key identifying characteristic: complete denial that there are security issues which genuinely affect the business. Often conspiratorial.	Obsession with buying the “best” product, usually without any definition of “best”.	Complete focus on meeting and auditing against compliance requirements.	No more “secure/insecure” dichotomy, but the heavy use of risk and governance language during security discussions.	They understand that they likely already have attackers on their network, and the aim is to find and prevent them doing damage.	Assurance customers habitually engineer for failure, prefer or require independent validation of security claims, and often have multi-level (classification) networks.
No buying decision is made.	The buying decision is usually made by a generalist IT or (worse) an executive member, with no domain experience.	Decisions often made in legal or finance, with some input from IT as they have to implement.	Decisions made by specialist IT security staff, but often more in the architectural than operational domain.	Decisions spread across architectural and operational teams, usually fronted by a CISO or CIO who makes the final call.	Purchase decision is often made by highly technical teams, with a layer of procurement /project/vendor management assisting.

OSI Layer 8 and Layer 10 Attacks

- Unfortunately, the endpoint which causes us the most problem remains the one sitting between the keyboard and chair (PBKAC, or the “Layer 8” vulnerability)
- Security training is essential, but humans are too unpredictable and inconsistent for it to be more than 90% effective (at best!)
- We also must resist layer 10 attacks: government or other bodies mandating insecurity:
  - How many more times will the Clinton-era export controls cause modern SSL/TLS problems?
  - Wikileaks “Vault 7” breach shows CIA hoarding vulnerabilities to use as weapons, now out in the open



Gigamon®

Ten Predictions for the Next Ten Years

Disclaimer

PULLING OUT THE INFOSEC CRYSTAL BALL

- The following are predictions, and not certainties
- They are presented here to promote discussion and thought around these possible challenges and solutions
- Each is categorized by:
  - Expected timeframe
  - Confidence:
    - Possible (25%+)
    - Likely (50%+)
    - Very likely (90%+)

Predictions

2017-2027

Prediction 1

- “Clean Feeds” supporting the detection and quarantining of insecure IoT devices will become standard
- Expectation: 3-5 years
- Confidence: likely

Prediction 2

- IoT product vendors will be forced by legislation to take responsibility for the issues caused by their products
- Expectation: 5 years+
- Confidence: likely

Prediction 3

- Targeted Ransomware aimed at high net-worth and highly placed individuals and institutions
- Expectation: 0-2 years
- Confidence: very likely

Predictions

2017-2027

Prediction 4

- Levels of encryption inside financial organizations is going to asymptotically approach 100% over the next ten years
- Expectation: 0-10 years
- Confidence: very likely

Prediction 6

- Banks which see security as an architectural problem, rather than an operational one, will suffer significant financial losses
- Expectation 1-3 years
- Confidence: very likely

Prediction 7

- Any Financial Organization whose Security Operations Centre doesn't have total visibility of their network has intruders hiding in the invisible areas
- Expection: now
- Confidence: very likely

Predictions

2017-2027

Prediction 8

- A Nation-State will perform an attack upon a foreign bank, as a part of a cyber-offensive campaign against that bank's country. In doing so, they will release a large trove of very embarrassing internal documentation, which will cause that bank significant reputational damage and financial impact.
- Expectation: 1-3 years
- Confidence: very likely

Prediction 9

- We will see attacks against banks using nation-state like "implants", delivered into the bank using the supply chain
- Expectation 1-3 years
- Confidence: very likely

Prediction 10

- Financial companies will continue to deploy an increasing number of applications to the cloud
- Expectation: 1 year
- Likelihood: very likely (already happening)

Predictions

2017-2027

What happened to prediction 5?

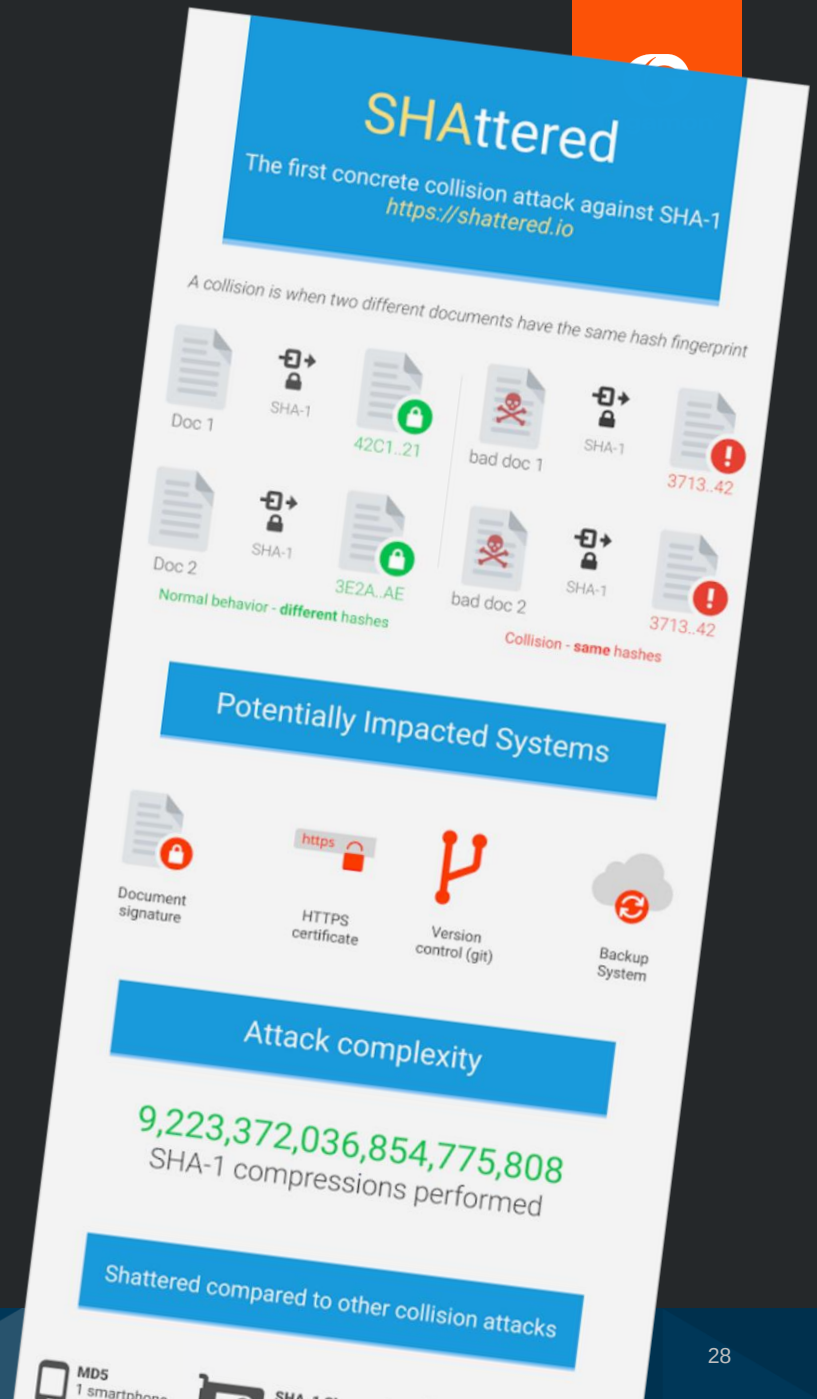
Predictions

2017-2027

Prediction 5

- We'll see more cryptanalytic findings against hash functions, and SHA-1 won't be the last we need to deprecate
- Expectation: 5-10 years
- Confidence: likely

- This was written in Dec 2016, when SHA-1 had been being deprecated for years.
- Then this happened, and we now need to move FAST.
- Designing strong hash functions turns out to be hard, but they're the basis for digital signatures (and certificates). So far MD2, MD4, MD5, SHA-0 and SHA-1 have all fallen. Likely they're not the last.



Revision History

DOCUMENT STATUS: RELEASE

Author	Status	Ver	Date	Comments
Ian Farquhar	RELEASE	1.0	14-MAR-2016	First release.