RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M04

INTRODUCTION AND A LOOK AT SECURITY TRENDS

Hugh Thompson, Ph.D.

Program Committee Chairman, RSA Conference


WELCOME TO THE PADANGTEGAL
MANDALA WISATA WANARA WANA
SACRED MONKEY FOREST SANCTUARY
DEAR VISITORS,
ON BEHALF OF THE VILLAGE OF PADANGTEGAL AND THE WANARA WANA FOUNDATION WE WISH YOU AN ENJOYABLE AND EDUCATION VISIT TO OUR FOREST SANCTUARY AND TEMPLE COMPLEX. TO ENSURE A TRULY PLEASURABLE VISIT PLEASE OBSERVE THE FOLLOWING:
1. THIS IS A SACRED AREA. PLEASE COMFORT YOURSELF WITH RESPECT FOR THE PEOPLE WHO WORSHIP HERE, THE TEMPLES AND THE MONKEYS AND OTHER PLANTS AND ANIMALS THAT RESIDE IN THE FOREST
2. THE MONKEYS OF THIS FOREST ("KERA" OR "MACHQUES") ARE FREE LIVING WILD ANIMALS PLEASE REFRAIN FROM TOUCHING OR PLAYING WITH THEM AS THEY MAY REACT IN AN UNPREDICTABLE MANNERS. DO NOT PROVIDE PEANUTS FOR THE MONKEYS AS THEY ARE A POTENTIAL HEALTH RISK. SEEK OUT A STAFF MEMBER (GREEN SARONGS) FOR ANY ASSISTANCE REGARDING THE MONKEYS
3. PLEASE READ THE BROCHURE PROVIDE WITH THE ENTRANCE TICKET FOR FURTHER INFORMATION ABOUT THIS SANCTUARY
WE THANK YOU FOR FOLLOWING THESE REGULATIONS AND WE TRUST THAT YOUR VISIT WILL BE A MEMORABLE ONE
SINCERELY,
WANARA WANA FOUNDATION


RISK

Agenda

- Intro to Information Security
- Economics of Information Security
- Security Trends

The Shifting IT Environment

(…or why security has become so important)

Shift: Compliance and Consequences

- The business has to adhere to regulations, guidelines, standards,…
  - SAS 112 and SOX (U.S.) – upped the ante on financial audits (and supporting IT systems)
  - PCI DSS – requirements on companies that process payment cards
  - HIPAA, GLBA, GDPR, …, many more
- Audits have changed the economics of risk and create an “impending event”

Hackers *may* attack you but auditors *will* show up

- Disclosure laws mean that the consequences of failure have increased
  - Waves of disclosure legislation

Shift: Technology

- Many applications/transactions now operate over the web
- Cloud has changed our notion of a perimeter
- Worker mobility is redefining the IT landscape
- Shadow IT is becoming enterprise IT
- Majority of web transactions are now encrypted (SSL)
- The security model has changed from good people vs. bad people to enabling partial trust
  - There are more “levels” of access: Extranets, partner access, customer access, identity management, …

Shift: Attackers

- Many cyber criminals are organized and profit-driven
  - An entire underground economy exists to support cybercrime
- Attackers are shifting their methods to exploit both technical and human weaknesses
- Attackers after much more than traditional monetizable data (PII, etc.)
  - State-sponsored attacks
  - Influence
  - Hacktivism
  - IP attacks/breaches

Shift: Customer expectations

- Customers, especially businesses, are using security as a key discriminator
- Security has become a non-negotiable expectation of businesses
- Security is being woven into service level agreements (SLAs)
- The “average person” is now familiar with security

Big Questions

- How do you communicate the value of security to the enterprise (and management)?
- How do you measure security?
- How do you rank risks?
- How do you reconcile security and compliance?
- How do you adapt to paradigms like IoT?
- How can you be proactive and not reactive? What is “threat intelligence” and how would you actually consume, act on or share it?
- What changes are likely in privacy laws, data sovereignty, trust?
- What about big issues in the news like breaches of very personal data that cannot be reset or revoked? How should/can we adapt what we do based on them?

The Economics of Security

Hackernomics (*noun*)

A social science concerned chiefly with description and analysis of attacker motivations, economics, and business risk. Characterized by

5 fundamental immutable laws and 4 corollaries

Law 1

Most attackers aren't evil or insane; they just want something

Corollary 1.a.:

We don't have the budget to protect against evil people but we *can* protect against people that will look for weaker targets

Law 2

Security isn't about security. It's about mitigating risk at some cost.

Corollary 2.a.:

In the absence of metrics, we tend to over focus on risks that are either familiar or recent.

Law 3

Most costly breaches come from simple failures, not from attacker ingenuity

Corollary 3.a.:

Bad guys can, however, be VERY creative if properly incentivized.

The CAPTCHA Dilemma

Completely

Automated

Public

Turing test to tell

Computers and

Humans

Apart

Law 4

In the absence of security education or experience, people (employees, users, customers, …) naturally make poor security decisions with technology

Corollary 4.a.:

Systems needs to be **easy to use securely and difficult to use insecurely**


Messana
GRATED
PARMESAN
CHEESE
Comet
MULTI-ROOM

Law 5

Attackers usually don't get in by cracking some impenetrable security control, they look for weak points like trusting employees

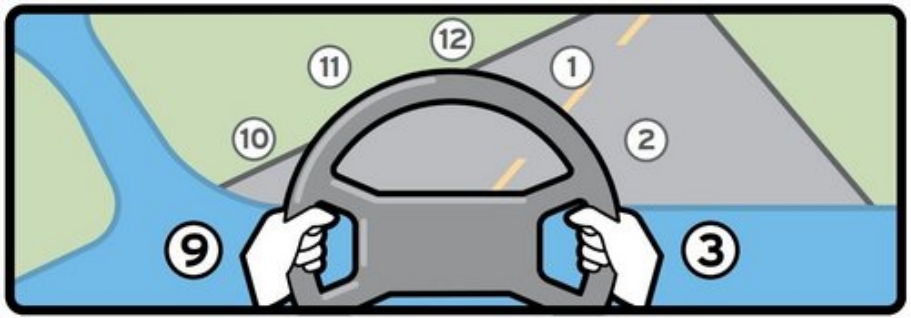
RSA Conference Submission Trends

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
web 2.0	web 2.0	data	real–world	BYOD	APT	BYOD	IoT	IoT	IoT
network access control	anti–virus	risk	real–time	tablet	BYOD	IoT	threat actors	ransomware	ransomware
anti–virus	social networking	organizations	cloud–based	APT	security analytics	security analytics	BYOD	devops	GDPR
cross–site scripting	cross–site scripting	access	third–party	anti–virus	mobile apps	threat actors	security analytics	threat actors	iot devices
PCI–DSS	PCI–DSS	compliance	in–depth	MDM	software–defined	home depot	kill chain	kill chain	devops
sarbanes oxley	myspace	key	high–profile	iOS	MDM	snowden	devops	GDPR	blockchain
service–oriented	conficker	attacks	real–life	stuxnet	iOS	software–defined	OPM	blockchain	equifax
unified communications	VOIP	applications	Epsilon	Flame	stuxnet	data science	software–defined	cyber insurance	wannacry
javascript	payment card	control	end–user	mobile apps	tablets	devops	NIST CSF	security analytics	threat hunting
management strategy	ratio	process	enterprise–wide	advanced malware	prism	heartbleed	iot security	NIST CSF	bitcoin
PDAs	security standard	enterprise	zero–day	kill chain	advanced malware	kill chain	anthem	dark web	deep learning
email security	data security	environment	cost–effective	software–defined	dropbox	ransomware	dark web	bitcoin	devsecops

Source: Cyentia Institute with data from RSA Conference

Some hot areas…

- GDPR and data privacy
- Data sovereignty and legislative volatility
- The human element of security
- The potential application of blockchain technologies to security
- The application, potential and limitations of AI in security


12
11
1
10
2
9
3

Enjoy the rest of the conference!!

THANKS!

Hugh Thompson, Ph.D.

hugh_thompson@symantec.com