

Transcending From Digital to Physical



Yaniv Simsolo, CISSP
CTO, Palantir Security



OWASP
Israel

Israel Chapter Meeting March 2015



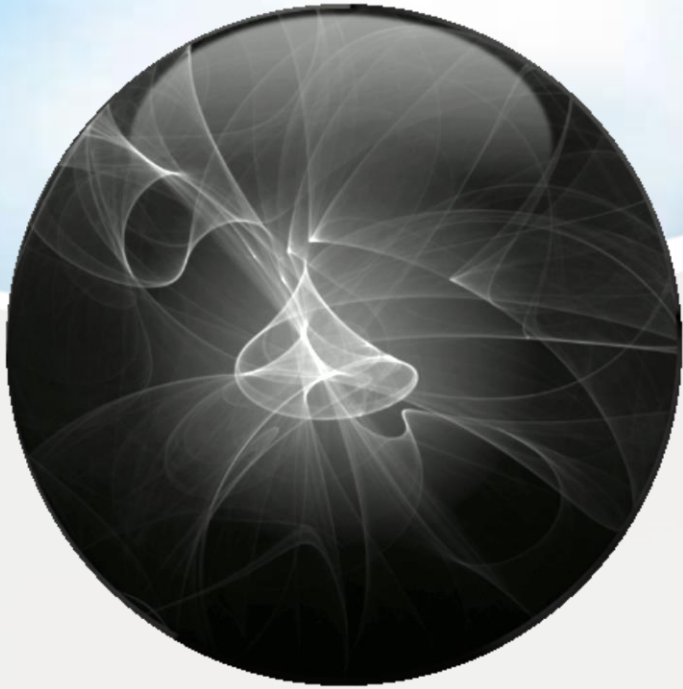
alantir
security

Agenda



- Typical showcases
- Trends in hacking and applications
- Transcending from digital to physical
- Conclusions

Transcending From Digital to Physical



Typical showcases



Once Upon a Time in Hackland

- Originally hacking concentrated on physical networks and infrastructure.
- The motivation: respect.

Once Upon a Time in Hackland

- When hacking moved into the application realm, the motivation changed.
- Getting to the physical realm went out of focus

Happily Ever After?

Every now and then though...



Once Upon a Time in Hackland



Source: YouTube

It's a New World

- SCADA
 - Public awareness grew with Stuxnet (2010)
 - Seminal security event
 - Worldwide ripple effect
- What if...
 - SCADA is just a means to an end

It's a New World

- Vehicle security is an issue
 - The information systems of the vehicle serve as the syringe
 - Attacking the physical realm through the digital
 - Public awareness grew after DefCon 2013



Source: YouTube

Digital Carjackers Show Off New Attacks

Transcending From Digital to Physical



Trends in Hacking and Applications



Trends in Hacking and Applications

- Social networks
 - חבר'יה – the first social network.
 - Once reaching the bandwagon effect, within 30 days...
 - Facebook hacking
 - Not all hacks are aimed at the digital realm
 - Simple robberies can benefit from Facebook



Introducing: Mr. Obvious

- History Recurrence - George Santayana observed that: "Those who cannot remember the past are condemned to repeat it.",

The Life of Reason, vol. 1:
Reason in Common Sense,
1905 (wikipedia).

יכר השבת האתר החדש

חדשות כלכלה - וידאו חרדים - חדשות - מזיקה - אוכל בריאות ברמה - י

TRADE24!

חדשות < דיגיטל < סלולר ואפליקציות < קיבלתם סמס מחברת החשמל? היזהרו, זו הונאה

קיבלתם סמס מחברת החשמל? היזהרו, זו הונאה

יצא לכם לקבל הודעת SMS מחברת החשמל הקוראת לכם לעדכן את אמצעי התשלום? החברה מזהירה כי מדובר בהונאה "לא נשלחה כל הודעה מטעמינו יש להתעלם"

חיים אבני | י' בסיון תשע"ד 08.06.14 22:29

הדפסה 23 אהבתי 1 ציוץ 0 +1 0

עדכן את כרטיס האשראי באמצעותו שילמת את חשבון החשמל שלך התראה לפני ניתוק

<http://nexti.co.il/www.israel-electric.co.il>

תחקיר דיגיטל

בקיצור, ניסינו לתקן

Introducing: Mr. Obvious

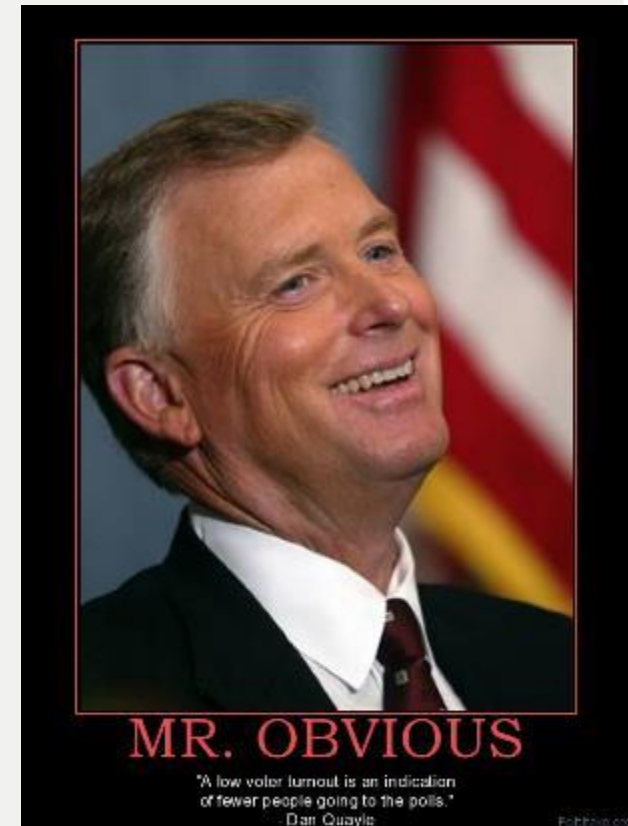
- The resurrection of SMiShing
- SMiShing – pre 2005 attack vector

Originally used as a SPAM attack vector in banking frauds.

Resurrected in a non-spam “business” model attack vector.

- **That an attack is OLD, does not mean it is dead!**

Source: politifake.org



Return of the Ransom

www.themarket.com/markets/1.2587294

כניסה TheMarker חיפוש ניווט

שוק ההון

יו"ר לאומי על פרשת הסחיטה בבנק: הפרסום יביא לכאוס במערכת הבנקאית

בחדשות 2 נחשף כי יו"ר לאומי ביקש להעניק חסינות פלילית לעובד שסחט את הבנק - בהתאם לדרישת הסוחר ■ המפקח על הבנקים: "חשש לאובדן אמון הציבור בבנק"

סיון איזקו | 20:06 11.03.2015

449 74 שמו

מכתב ששלח בנובמבר יו"ר בנק לאומי, **דוד ברודט**, לפרקליט המדינה, שי ניצן, חושף את הפאניקה שאחזה בצמרת הבנק השני בגודלו במדינה - לאחר שבסוף אוקטובר התקבל **מייל סחיטה מעובד** לשעבר בלאומי-קארד, שבו טען העובד כי הוא מחזיק במידע על מיליון וחצי לקוחות הבנק - כפי שנחשף הערב בחדשות ערוץ 2.

לאומי פנה מיד למשטרה, עירב את המפקח על הבנקים, דודו זקן, וקיים דיון בהול עם פרקליט המדינה - וזאת נוכח דרישתו של הסוחר לקבל לא רק דמי סחיטה, אלא גם התחייבות לחסינות מהליכים פליליים בנין מעשה הסחיטה.

האירוע, כך התברר, עורר בקרב בנק לאומי והמפקח חשש כבד מהסתערות המונית של לקוחות על הבנק. בדרישה להוציא את כספיהם נוכח החשש מקריסתו - עקב

הכתבות הנקראות באתר

כל המ שאתנ עליהב

"החשבון האיראני" בבנק ישראל התכווץ ב-64 מיליון דולר

בנק יע מיליא

עוני ותחלואה: החצר האחורית של ארה"ב

השקמה

TheCloud

תשואה של עשרות אחוזים

Consider Virlock

www.darkreading.com/hackers-breaking-new-ground-with-ransomware/d/d-id/1319475?

ATTACKS/BREACHES

3/13/2015
06:00 PM



Jai Vijayan
News

Connect Directly



2 COMMENTS
[COMMENT NOW](#)

[Login](#)

Hackers Breaking New Ground With Ransomware

The tools and tactics being used to go after victims reveal growing sophistication, and gamers need to look out, security researchers say.

The enormous success which hackers have had extracting millions of dollars from individuals and businesses using ransomware appears to be driving more sophisticated tools and tactics from them.

This week researchers sounded the alert on two recent ransomware families that break ground in different ways.

One of them dubbed Virlock is noteworthy because it not only locks the screen of compromised systems like other ransomware, but also infects files on the device. First noticed by security firm [ESET](#) in December, Virlock is also polymorphic, meaning the code changes every time it runs making it hard to detect using standard malware detection tools.

Trends in Hacking and Applications

- The defender's mission is easier.
 - ???

"On the Internet today, it is much easier to attack systems and break into them than it is to defend those systems against attack, so the advantage is to the attacker. This is true for a combination of reasons: the ability of an attacker to concentrate his attack, the nature of vulnerabilities in computer systems, poor software quality and the enormous complexity of computer systems."

Source: <https://www.schneier.com/blog>

Trends in Hacking and Applications

- Security is relative
- Most attacks are not specifically targeted
 - hackers attack whatever they can and hack what is feasible.

What if...

- Attacks are targeted?

Braking the perimeter

- Through authorized users – the Lockheed Martin Hack
- Determination - a key in locating the needle in the haystack.
- Mr. Ed Schwartz, VP and CISO, RSA, the Security Division of EMC: **“Recently we learned that two factor authentication is not enough anymore”**,
 - Managing Advanced Security Threats Using Big Data Analytics, International Cyber Conference II, Israel, June 2012



Bypassing a Closed Network

- The network is enclosed!
- Yep, but are **all** input channels or in put means protected?

Suter (computer program)

From Wikipedia, the free encyclopedia

Suter is a military computer program developed by BAE Systems that attacks computer networks and communications systems belonging to an enemy. Development of the program has been managed by Big Safari, a secret unit of the United States Air Force. It is specialised to interfere with the computers of integrated air defence systems.^{[1][*dead link*]} Suter was integrated into US unmanned aircraft by L-3 Communications.^[2]

Three generations of Suter have been developed. Suter 1 allows its operators to monitor what enemy radar operators can see. Suter 2 lets them take control of the enemy's networks and direct their sensors. Suter 3, tested in summer 2006, enables the invasion of links to time-critical targets such as battlefield ballistic missile launchers or mobile surface-to-air missile launchers.

The program has been tested with aircraft such as the EC-130, RC-135, and F-16CJ.^[1] It has been used in Iraq and Afghanistan since 2006.^{[3][4]}

U.S. Air Force officials have speculated that a technology similar to Suter was used by the Israeli Air Force to thwart Syrian radars and sneak into their airspace undetected in Operation Orchard on September 6, 2007. The evasion of air defence radar was otherwise unlikely because the F-15s and F-16s used by the IAF were not equipped with stealth technology.^{[3][5]}



Tools of the Trade

Misconception trends:

- We CAN test for security
- Our tools CAN scan the entire grounds
- Our protection tools CAN protect us
- We have a large security team = we ARE secured

Tools of the Trade

InfoSec Natural Selection, Shay Chen, OWASP IL 09_2014



#	Logo	Vulnerability Scanner	COUNT	COOKIE	POST	COOKIE	HEADER	SECRET	PARAM	XML	XMLATT	XMLTAG	JSSON	SCRIPT	AMT	JAVASER	SCRIPT	WCF	WCF-BI	Webser	DBWR	HTTPC	DIR	FILE	PARAM	XML	XML	JAVASER	MULTI	GWT	ODATA	ODATA
1		Burp Suite Professional	19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
2		IBM AppScan	17	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✗
2		NTOSpider	16	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗
4		WebInspect	13	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	
5		Netarker	9	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	
6		ScanToSecure		9	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗
7		Acunetix WVS		7	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
8		Armonix	7	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
9		Sylent Dynamic	7	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
10		N-Stalker		6	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗

Tools of the Trade

- Old news.
- We all know that the tools are not complete.
- Did we?

What if...

- just few are listening

Transcending From Digital to Physical



Transcending



Vehicle security is an issue

- Is it:
 - Application security?
 - Vehicle IT security?
- The real issue is: passenger and road safety.



Source: YouTube

Digital Carjackers Show Off New Attacks

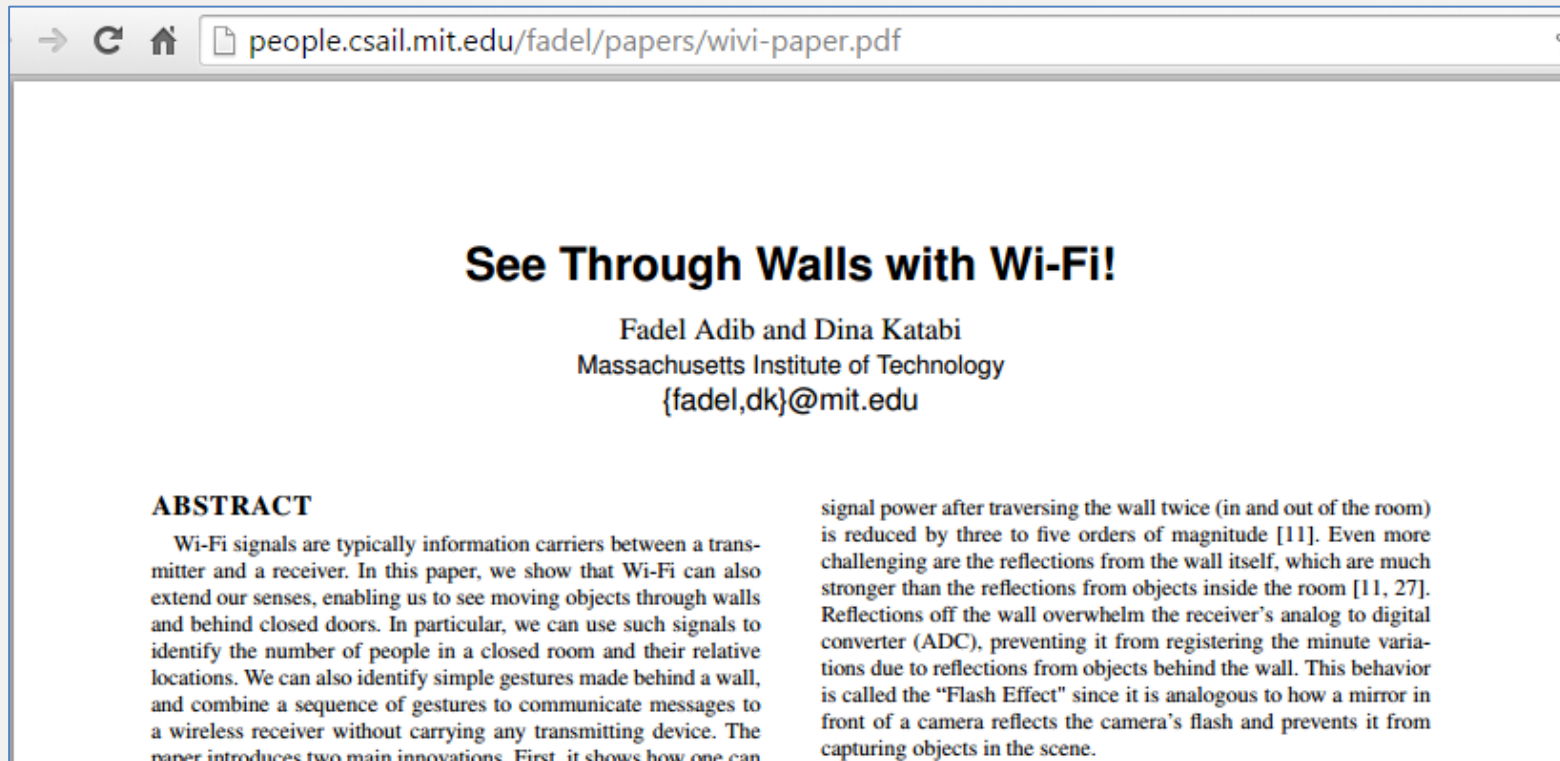
Sci-Fi Far-Fetched

- The Dark Knight cellphone sonar.
- Far Fetched?
- Requirements:
 - all phones access/connect
 - Vast computing power



Sci-Fi Far-Fetched

- MIT wi-fi radar – see through walls.
- Working model. Published documents.



The image shows a screenshot of a web browser window. The address bar at the top contains the URL `people.csail.mit.edu/fadel/papers/wivi-paper.pdf`. The main content area of the browser displays the title **See Through Walls with Wi-Fi!** in a large, bold, black font. Below the title, the authors' names, **Fadel Adib and Dina Katabi**, are listed, followed by their affiliation, **Massachusetts Institute of Technology**, and their email address, `{fadel,dk}@mit.edu`. The text is centered. Below the authors' information, there is an **ABSTRACT** section. The abstract text is left-aligned and describes the paper's contribution to Wi-Fi technology, specifically its ability to see through walls and behind closed doors by using signal reflections. The abstract is split into two columns.

ABSTRACT

Wi-Fi signals are typically information carriers between a transmitter and a receiver. In this paper, we show that Wi-Fi can also extend our senses, enabling us to see moving objects through walls and behind closed doors. In particular, we can use such signals to identify the number of people in a closed room and their relative locations. We can also identify simple gestures made behind a wall, and combine a sequence of gestures to communicate messages to a wireless receiver without carrying any transmitting device. The paper introduces two main innovations. First, it shows how one can

signal power after traversing the wall twice (in and out of the room) is reduced by three to five orders of magnitude [11]. Even more challenging are the reflections from the wall itself, which are much stronger than the reflections from objects inside the room [11, 27]. Reflections off the wall overwhelm the receiver's analog to digital converter (ADC), preventing it from registering the minute variations due to reflections from objects behind the wall. This behavior is called the "Flash Effect" since it is analogous to how a mirror in front of a camera reflects the camera's flash and prevents it from capturing objects in the scene.

Sci-Fi Far-Fetched



New system uses low-power Wi-Fi signal to track moving humans — even behind walls

'Wi-Vi' is based on a concept similar to radar and sonar imaging.

Helen Knight, MIT News correspondent
June 28, 2013

▼ Press Inquiries

RELATED

Sci-Fi Far-Fetched



Can Wi-Fi let you see people through walls? yes it definitely can. Wi-Fi is a signal, basically like a sonar that bounces off of every thing it encounters, as we saw in the film the Dark Knight.

Researchers at MIT have developed a sensing technology that uses low-power Wi-Fi to detect moving people behind walls. The system is next gen technology compared to other wall-penetrating radars that utilize heavy equipment.

The Wi-Vi system by Dina Katabi and Fadel Adib sends out a low-power Wi-Fi signal and tracks its reflections to sense people moving around, even if they're in closed rooms or behind walls. The MIT system can be set to view or ignore stationary objects or simply focus on moving people . It can determine the number of moving persons in the room and their relative locations.



Sci-Fi Far-Fetched

Wi-Vi: See Through Walls
with Wi-Fi Signals



Sci-Fi Far-Fetched?

- Is there a fundamental difference?
- The technology is in the private sector.



Personal View

Act 1

- Recently



Personal View

Act 2

- Ah! The Piles!
- Mitigation is in order



Personal View

- Barricade



Personal View

- Deter



Personal View

- Alert (silent, non-silent)



Personal View

- Risk Transfer



Personal View

What if...

- Analyzing: threat analysis Vs. estimated mitigations costs.
- The results are not that funny.



Personal View

Act 3

- Surprising Twist
- What to do with all this information?
- Allocate extra resources

Internet of Things

- IoT definition: *“the network of physical objects or “things” embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices”*. (wikipedia)
- *“Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure”*

Internet of Things

- Great! I want some now!



Internet of Things

What if...

- No way ever that I am going to have a LAN router and LAN lines to ALL the devices of internet of things at home.
- Obvious solution: Wi-Fi.

Internet of Things

- Security is relative
- Do I really have the resources and will to spend them protecting my home appliances?
 - The laundry machine
 - The refrigerator
 - The deep freezer
 - The TVs
 - The DVD/VCR/TV Decoder
 - The Radio/Multimedia
 - The musical electrical instruments
 - The garden/plants watering computer
 - Computers, Backups, Streamers
 - Windows and electricity shutters
- What about other sensors?



Internet of Things

- Security is relative
- Do I really know all the sensors I have at home?
 - WiFi
 - Video
 - Audio
 - Temperature
 - Location
 - Other Sigint and Comint?

Source: The hacker news

China is planting spying microchips in Electric Iron and kettles that can scan Wi-Fi devices to serve malware

Friday, November 01, 2013 Pierluigi Paganini

401 Like 2.7k Share 4495 Tweet 674 Reddit 1498 Share 229

ShareThis 8810



Internet of Things

- The protection required: SSL, authentication, authorization, separation of duties, segmentation of my home network
- Additional protection: compartmentalizing my computers, from my phones, from my home appliances, from my Tablets, from my cars, from my TVs, from my streamers
- Am I nuts?



Internet of Things

- The “things” should support secured protocols.
- KMS – key management solution

Internet of Things

What if...

- Assuming: Wi-Fi, SSL everywhere
- Can SSL everywhere be trusted?



Solution Brief

Safely Expand SSL/TLS for Data Protection



[DOWNLOAD NOW](#)

Data privacy, increasing cyber attacks, and Google's prioritization of HTTPS have dramatically increased the use of SSL/TLS. But pervasive SSL/TLS only addresses data security if the keys and certificates are securely managed and protected.

Cost of Failed Trust

- The world is rapidly moving to SSL everywhere and certificates everywhere solutions.
- What if...
 - trust is lost?
 - You cannot trust your own connections?



The Ponemon Institute's *2015 Cost of Failed Trust Report* reveals most organizations believe the trust established by cryptographic keys and digital certificates, which they require for their businesses to operate, is in jeopardy.

Cost of Failed Trust

- Organizations and individuals transfer risks often.
 - Credit Card industry
 - Individuals don't care
- Failed trust => transferring the risk will not be an option.



Cost of Failed Trust

- Attacks and security failures can cross the border from the digital to the physical realm.
- Once trust is failed => no one takes responsibility



www.autoevolution.com/news/four-dead-due-to-toyota-stuck-accelerator-pedal-11598.html

tion NEWS CARS MOTO REVIEWS SPYSHOTS GREENIQ Se

EDITORIAL COVERSTORY AUTO SHOWS STARS & CARS TUNING AUTO HOW-TO BAC CAL
A MERCEDES

Four Dead Due to Toyota Stuck Accelerator Pedal

SHARE:  SHARE  SHARE  TWEET

Q The safety glitch we told you about yesterday killed no less than four people in the United States. At least, this is the only accident we heard about at this time, although preliminary reports are claiming more than 100 incidents occurred in either Toyota or Lexus models.

Transcending From Digital to Physical



Conclusions



Cloudbots

- Hosting abomination has arrived
- Cloud botnets in the wild
- Unlimited by Moore's law

www.darkreading.com/researchers-create-legal-botnet-abusing-free-cloud

Researchers Create Legal Botnet Abusing Free Cloud Service Offers

Hack depends on scripts creating scores of unique email addresses and automating execution of email verification

Last week at the RSA Conference, a pair of researchers demonstrated how it was possible to legally create a botnet for free by abusing trial accounts made available by high-powered platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) offerings.

"We were curious if we could build a botnet out of freely available cloud services," said Rob Ragan, senior security associate for Bishop Fox, who has been experimenting on that premise for the past several years with his colleague Oscar Salazar, security associate at Bishop Fox. "We started getting all these emails and alerts of, 'Here's a free Amazon EC2 box, there's free storage space, here's a free platform to develop and host your code.' We thought, 'Wow! That is a lot of computing power for free.'"



[Click here for more articles about the RSA Conference.](#)

www.wired.com/2014/07/how-hackers-hid-a-money-mining-botnet-in-ar

WIRED

How Hackers Hid a Money-Mining Botnet in the Clouds

HOW HACKERS HID A MONEY-MINING BOTNET IN THE CLOUDS OF AMAZON AND OTHERS



Relativity

- Security is relative.
- Architectures advancement:
 - Mainframes
 - Two tier
 - Three tier
 - Multi tier / Compound / Hybrid
 - Smart Phones
 - Cloud
 - IoT
 - Wearables
 - Us!

History Repeating

- 2010 – Privacy is dead
- RSA conference 2011 – in depth security is dead.
- RSA conference 2012 – security is dead.
- What's next?

History Repeating

- My Identity is public, no longer mine:
 - ID's are common knowledge,
 - Habits are rated and categorized for decades by EVERYONE (credit companies use this to detect anomalies for example)
 - My biometric is already partially exposed
 - Medical records on the web,
 - Biometric database is bound to leak,
 - My face is recognized by so many entities with face recognition Capabilities,
 - Dental records...
- What's next?

Typical Software Development



How the customer explained it



How the Project Leader understood it



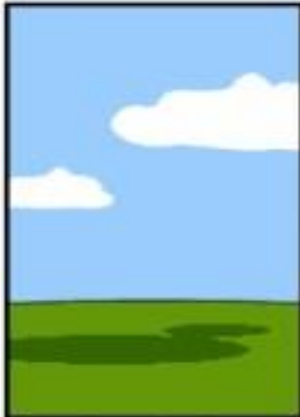
How the Analyst designed it



How the Programmer wrote it



How the Business Consultant described it



How the project was documented



What operations installed



How the customer was billed



How it was supported



What the customer really needed

Typical Software Development

- In a field of over-complexity, each decision may be the security-crucial one.
- Common decisions:
 - “no more than X medium bugs, no more than Y high bugs is OK for Production”
 - “testing certain part of a system is out of scope”
- Are such decisions acceptable?
- For some systems it is already too late

History Repeating - Safety

- Updated reality: Safety is relative
- Yep! I trust this car's safety AND security!



חדשות רכב

המכונית תניע, רק אם תזהה את הנהג

חברת אינטל ויצרנית הרכב פורד מפתחות מערכת זיהוי פני הנהג, שתאפשר התנעה רק אם היושב מאחורי ההגה מורשה. אם לא, תמונתו תישלח מיד לבעל הרכב

רועי צוקרמן | סדרים: 09:30, 30.06.14

Recommend 41

פורד וחברת הטכנולוגיה אינטל מפתחות מסוכנת חכמה, שתזהה את הנהג הנכנס אליה באמצעות מצלמה ותוכנת זיהוי פנים. במידה והנהג אינו מופיע ברשימת המורשים לנהיגה, המכונית לא תניע ותשלח את תמונת ה"פולש" לטלפון הנייד של בעל הרכב.

הטכנולוגיה, שמפותחת בסיוע מרכז המחקר ופיתוח של אינטל בישראל, תאפשר לצמצם את הסיכון לגניבת הרכב, ותציע לבעל המכונית שורה של אפשרויות שליטה חדשות. בין היתר הוא יוכל לקבוע את מהירות הנסיעה המרבית של הרכב באמצעות יישומן סלולרי, להגביל את עוצמת מערכת השמע ולמנוע שימוש בטלפון נייד בזמן נהיגה - למשל במקרים בהם נהג צעיר מקבל את המפתחות.

2014 Ford Fiesta | פורד פיאסטה



קרקע חלקאית באזור פרדס חנה

הבית שעליו חלמת במרחק נגיעה

עם יעד מאושר למטרים 10 לפרטים <<<<

History Repeating

- *"Twenty five drivers start every season in Formula One, and each year two of us die. What kind of person does a job like this? Not normal men, for sure. Rebels, lunatics, dreamers. People who are that desperate to make a mark, and are prepared to die trying."* Niki Lauda quote from the movie Rush
- Remember Boeing 787 special condition warning?
- What's next?

History Repeating

- How Will the relevant car-control app
 - be secured?
 - Be private?
- Is it really safe to limit the car speed to 100 kph?
- Imagine Resource Depletion attacks (e.g. Syn flood) on the car's safety systems

The Lacuna

- Lacuna definition, Wikipedia: “In law, a *non liquet* is a situation where there is no applicable law. Non liquet translates into English from Latin as “it is not clear.”
- (some) Law and governments have long learned that (some) Lacunas can be a good thing.
- LAW relates to REAL life, where there will always be surprises and unplanned events.

The Lacuna

- However, in computer systems we DO wish to control everything.
- Computer systems are not flexible...

What if...

- Controlling everything is already here?
- Social networks show that in certain circumstances information systems ARE real life.

The Jinni is Leaving the Bottle

The essence of entropy:

- In the physical realm we actually need to be able not to decide and not to control everything.
- Hence, only hackers will have the Lacuna privilege, the rest of us will have quiet gray and boring life.



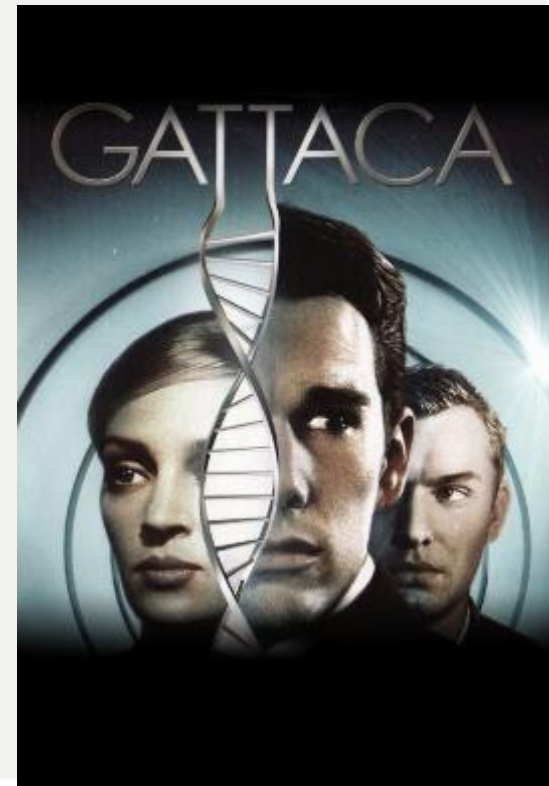
The Jinni is Leaving the Bottle

- It is becoming popular to discuss ways to tap into the mind or thought processes.
- Reconsider the Relativity Paradigm: it is much easier to attack than to protect...
- Historic Recurrence? Imagine Resource Depletion attacks on my thoughts.
- Do I really think my IQ can be reduced any more?



The Jinni is Leaving the Bottle

- So, in a short while some entity will categorize everything about me (probably already happened) AND everything that IS me.
 - Will we be able to extend our limits?
- Probably, by hacking...



The Point of No Return

- Food for thought - did we pass the Point of No Return?
- The Kasparov vs. Deep Blue More
 - Modern cloud chess systems
- The over-complexity and extended IT capabilities
 - Beyond the single individual's capabilities.
- Somewhere, those in control of the macro strategy estimate that individual organizations and individuals within organizations have control of computer systems.
 - Is that paradigm still intact?

The Jinni is Leaving the Bottle

- In the past we were not completely digitally-dependent
- We are now overwhelmingly digitally-dependent. All aspects of our lives are digital.
- Reconsidering history recurrence and the relativity of security, major changes are required.
- Passing the point of no returns calls for a revolution. Evolution is not sufficient.



Q&A

