אבטחה במערכות תעשייתיות

גיל קיני

gil@trinity.co.il

09-7677880

Trinity
Software & Beyond

מי אני? ולמה אני פה?

- **גיל קיני**
  - מעל 20 שנות ניסיון באבטחה, תוכנה וניהול
  - זמן-אמת, מערכות משובצות, תקשורת ו- VoIP
  - תהליכי פיתוח מכווני אבטחה כולל הנדסת-מערכת, תיכון וארכיטקטורה מאובטחת
  - פיתוח אלגוריתמים
  - שיפורי ביצועים למערכות קיימות
  - מחקרי אבטחה וכשלים
  - אבטחה ברמת מערכת

Trinity
Software & Beyond

מטרות ההרצאה

אבטחה במערכות תעשייתיות

- להעלות מודעות
- להוציא משאננות
- להסביר ולכוון

Trinity
Software & Beyond

Agenda

- אבטחת-מידע ⇔ אבטחת-מערכות
- בעיות אבטחה והשפעתן על הלקוחות והיצרנים
- מושגי יסוד ומושגים נפוצים
- התקפות – מי? למה? איך?
- דרכי התמודדות

אבטחת-מידע

⇕

אבטחת-מערכות

Trinity
Software & Beyond

מה ההבדל בין עֹוגה ועוגָה?

- שיטות ונהלים להגנה על <השלם-את-החסר> כנגד גישה לא מורשית, שימוש לרעה או ביצוע שינויים
- רמת או "מיקום" ההגנה (או לחילופין ההתקפה)
  - רשת / מערכת / מכשיר / אפליקציה / מידע

Juliet: What's in a name?
that which we call a rose
By any other name would
smell as sweet
- Act II, Scene 2

Trinity
Software & Beyond

אבטחה במערכות משובלצות

- Embedded system security much more dangerous & costly than traditional software vulnerabilities
  - Experts say embedded device manufacturers too often lack maturity when it comes to designing secure embedded systems
- **Security as a New Dimension in Embedded System Design**

Trinity
Software & Beyond

Embedded Systems

- Increasingly used in critical sectors
  - Defense, medical, power, comm, …
- Malicious and accidental failures can have dire consequences
- Embedded systems are not “all hardware”
  - They have software too ☺
- Autonomous nature

Trinity
Software & Beyond

Interconnected Network

- Embedded system are a complex network of components
- Components might be hardware or software
- Source code might be available for some components
- COTS components (only binary available)
- Failure can create cascading events

Trinity
Software & Beyond

Embedded Systems Are …

- Varied
  - Low end: cellphones, sensors, smartcards
  - Mid range: routers, home appliances
  - High end: telecom, mil\aero, meditech
- Interactive with physical world
- Pervasive in our daily life
- Essential for national critical infrastructure
- Migrating
  - From proprietary solutions to open standard
  - From standalone systems to networked environments

Trinity
Software & Beyond

Embedded Systems Challenges

- Security solutions developed in the context of desktop-based operating systems and networks
  - Mostly insufficient to secure embedded systems
- Designing secure embedded systems faces unique challenges
  - Embedded system design is a systems-software co-design problem
    - needs to meet cross-cutting requirements in terms of performance and physical constraints
  - More issues than what are addressed for desktop computing
    - Resource constraint
    - Development model and environment
    - Update model

Trinity
Software & Beyond

Control System Security

- The prevention of intentional or unintentional interference with the proper operation of industrial automation and control systems
- These control systems manage essential services including electricity, petroleum production, water, transportation, manufacturing, and communications

בעיות אבטחה
והשפעתן על הלקוחות והיצרנים

Trinity
Software & Beyond

הסכנות בכשלי אבטחה

- בטיחות
- השפעות סביבתיות
- בעיות בקו הייצור
- נזק למכשור / ציוד
- גניבת מידע
- תדמית החברה
- השפעה על מכירות וחוזים עתידיים

Trinity
Software & Beyond

בעיות אבטחה בסקטורים השונים

- מיכשור רפואי
- טלקום ותקשורת
- תעשיית הרכב
- בקרה תעשייתית
- פיננסים וביטוחים
- צבאי ותעופתי

Trinity
Software & Beyond

אבטחה בסקטור הרפואי

- "Hacking Medical Devices for Fun & Insulin"
  - In October 2011, Jack succeeded in overriding an insulin pump's radio control and its vibrating alert safety feature, demonstrating the dumping of a potentially lethal dose of insulin without the pump alerting a wearer
- "Implantable Medical Devices: Hacking Humans"
- "How to kill a man at 30 feet by hacking his pacemaker"
- "60 Minutes" interview - doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking

Trinity
Software & Beyond

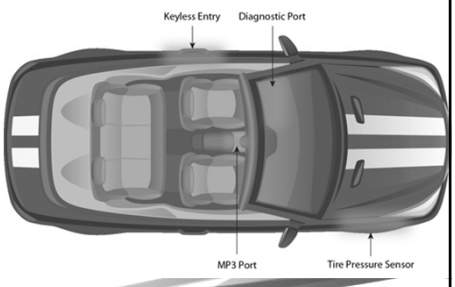
אבטחה בסקטור התקשורת

- Fraud
  - Revenue loss
- VoIP
- As attack on Critical National Infrastructure

Trinity
Software & Beyond

אבטחה בסקטור הרכב

- Take over the steering, acceleration, breaks and other important functions
- Drive-by Hacking via WiFi
- Hacking Cars with MP3 Files
- XM Radio
- In the near future
  - OS in cars – Android !



אבטחה בתשתיות תעשייתיות

- Iran has hacked US oil, gas and power companies
  - According to the WSJ the hackers were able to gain access to control-system software "that could allow them to manipulate oil or gas pipelines“
- Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent
  - A company whose software and services are used to remotely administer and monitor large sections of the energy industry
- חברת החשמל לישראל

אבטחה בסקטור הפיננסי

- As attack on Critical National Infrastructure
- Hacktivists
- APTs

Trinity
Software & Beyond

אבטחה בסקטור צבאי / תעופתי

- Similar to automotive?
- Researcher hacks aircraft controls with Android smartphone
- Iran – capturing the monster from Kandahar
- Natural evolution of ECM

מושגי יסוד ומושגים נפוצים

Trinity
Software & Beyond

Terms – Hacking Related

- Hacker
  - (Originally) A person who enjoys exploring the details of computers and how to stretch their capabilities
  - Cracker - One who breaks security on a computerized system
  - Black-Hat \ White-Hat
  - Script-Kiddies
- Hacktivism \ Anonymous \ LulzSec
  - A loosely affiliated collective of "hacktivists"
  - Ideologically motivated cyber attacks
    - motivated by perceived violations of social, political or environmental norms
    - Against corporate and governmental targets
    - Web site disruptions and defacements
    - Theft and release of sensitive documents & personal information

Trinity
Software & Beyond

Terms – Failures

- Back Door
  - A hole in the security of a computer system deliberately left in place by designers or maintainers
- Bug
  - An unwanted and unintended property of a program or piece of hardware, especially one that causes it to malfunction
- Buffer Overflow
- Vulnerability
  - A weakness that attackers or their malicious programs may be able to exploit

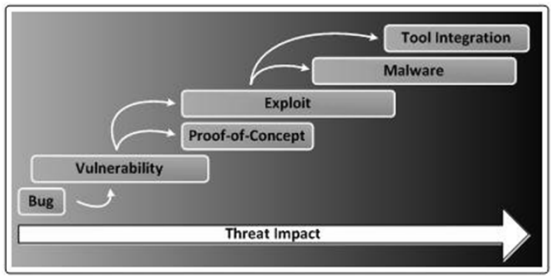
Trinity
Software & Beyond

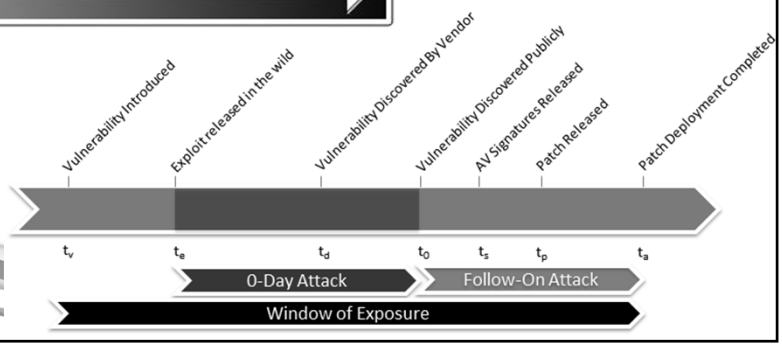
Terms – Offensive

- Attack
  - An attempt to bypass security controls on a computer. The attack may alter, release, or deny data
- Denial of Service (DoS)
  - DDoS
- Exploit
  - Code that is designed to take advantage of a vulnerability
- Fuzzing
  - שליחת הודעות שגויות, באופן מבוקר
  - במטרה להכשיל את המערכת תחת בדיקה
  - לשם מציאת נקודות כשל

Trinity
Software & Beyond

From Vulnerability to Exploit





Trinity
Software & Beyond

Terms – APT

Advanced Persistent Threat

- Usually refers to a group, such as a government, with both the capability and the intent to persistently and effectively target a specific entity.
- Commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques
- Recognized attack vectors include infected media, supply chain compromise, and social engineering
- Individuals, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target

Trinity
Software & Beyond

Terms – APT more…

- Advanced – operators have a full spectrum of intelligence-gathering techniques at their disposal. Often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it
- Persistent – operators give priority to a specific task, rather than opportunistically seeking information. The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. One of the operator's goals is to maintain long-term access to the target, in contrast to threats who only need access to execute a specific task
- Threat – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well funded

Trinity
Software & Beyond

Terms – Defensive

- Audit
- Perimeter Based Security
  - Firewall
  - IDS \ IPS
- Application Level Security
- Application Signing (or 'code signing')
  - Needs an application loader – itself a target
  - In-memory attacks
- Application Wrapping (aka Application Packing)
  - Needs unpacking at run-time
  - No protection of the application

Trinity
Software & Beyond

Terms – Confusing & Orphan

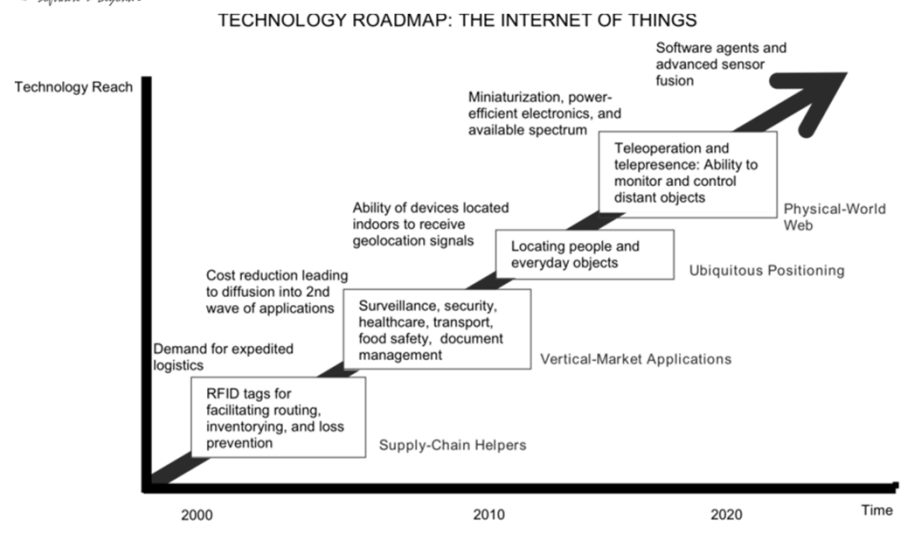
- Jail-Break
  - iOS jailbreaking is the process of removing limitations on iOS, on devices running it, through the use of software and hardware exploits; Jailbreaking is a form of privilege escalation
- Rootkit
- Anti-Virus
  - Signatures only
- Digital Signature
- PCI (Compliance)
- Penetration Testing
  - The portion of security testing in which the evaluators attempt to circumvent the security features of a system

Trinity
Software & Beyond

Terms – Internet of Things (IoT)

- Cyber / Cyberspace
- Internet of Things (IoT)
  - Refers to uniquely identifiable objects and their virtual representations in an Internet-like structure
- All is equal under heaven
  - *Tianxia*
    A phrase in the Chinese language and an ancient Chinese cultural concept that denoted either the entire geographical world or the metaphysical realm of mortals

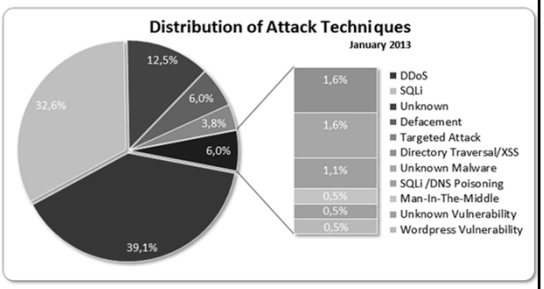
Trinity
Software & Beyond



Trinity
Software & Beyond

Terms – Attacks

- Phishing
  - A social engineering technique where cyber attackers attempt to fool you into taking an action in response to an email
  - Spear-Phishing
  - Whaling
- POS RAM-Scraper
- IP Theft
- Re-Packaging
- Attack Surface
- Pivoting



Trinity
Software & Beyond

Terms – Malware

- Virus
  - A type of malware that spreads by infecting other files, rather than existing in a standalone manner.
  - Usually spread through human interaction
- Worm
  - Can propagate automatically, typically without requiring any human interaction
- Trojan
  - "Trojan Horse“ - this type of malware appears to have a legitimate or at least benign use, but masks a hidden sinister function
- Spyware
  - Designed to spy on the victim's activities, capturing sensitive data
- Ransomware
- Cyber Weapon

Trinity
Software & Beyond

Terms – Industrial Networks

- **SCADA** (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition)
  - A process control application or system that collects data from sensors and machines locally or in remote locations and sends them to a central computer for management and control
- **Modbus** is a serial communications protocol
  - Originally published in 1979
  - For use with programmable logic controllers (PLCs).
  - Simple and robust, it has since become a de-facto standard communication protocol, and it is now a commonly available means of connecting industrial electronic devices.
  - developed with industrial applications in mind
  - Enables communication between many (approximately 240) devices connected to the same network, for example a system that measures temperature and humidity and communicates the results to a computer.
  - Often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (**SCADA**) systems

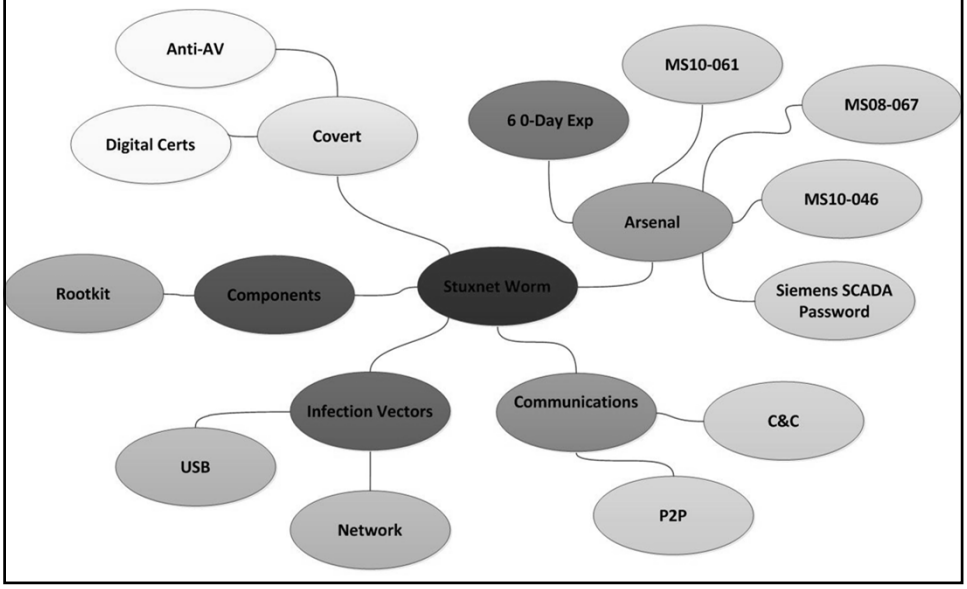
Trinity
Software & Beyond

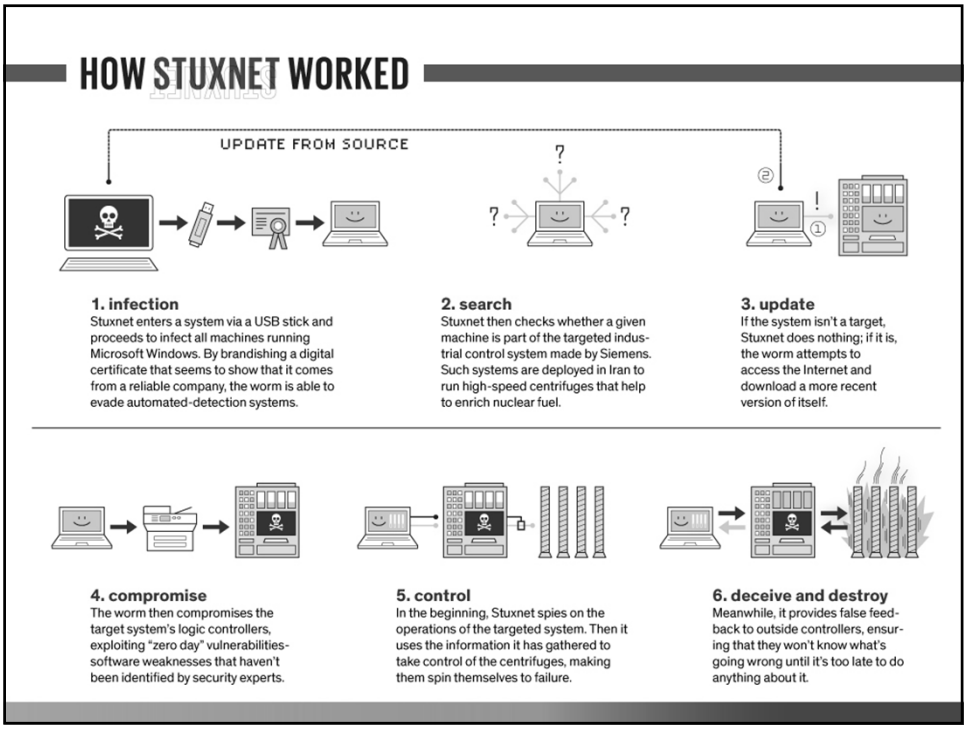
Stuxnet

- The first known custom-made virus designed to specifically infiltrate SCADA
- A sophisticated computer attack discovered in July 2010 that targeted control systems used to operate industrial processes in the energy, nuclear and other critical sectors. It was designed to attack Siemens Step7 software running on a Windows operating system exploiting a combination of vulnerabilities to gain access to its target and modify code to change the process.
- Stuxnet primarily targeted Siemens SCADA systems used in the Iranian uranium enrichment program

Trinity
Software & Beyond

Stuxnet Worm: Art of Cyber Warfare

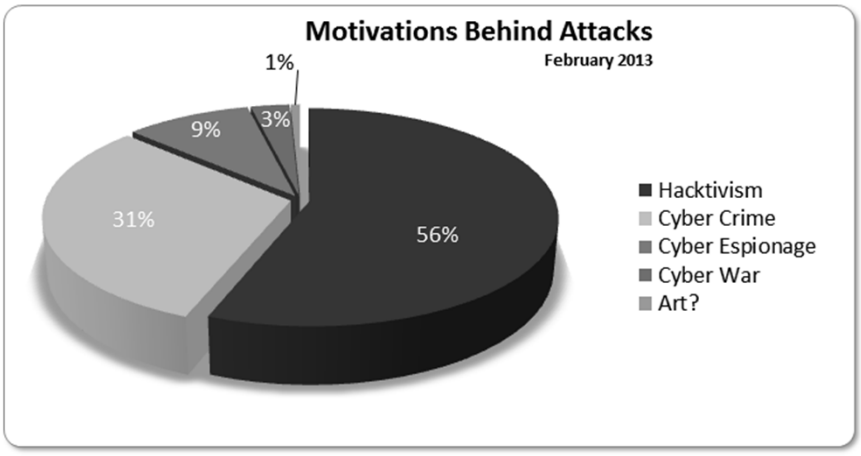




התקפות – מי? למה? איך?

Trinity
Software & Beyond

למה תוקפים?



Trinity
Software & Beyond

Types of Attackers

- Level 1: Script Kiddies
  - Essentially bored teenagers
- Level 2: The Hacking Group
  - Best described as a loose collection of script kiddies
- Level 3: Hacktivists
- Level 4: Black Hat Professionals
  - Their expert coding skills and determined attitude means they are often successful at attaining their target
- Level 5: Organized Criminal Gangs
- Level 6: Nation States

Trinity
Software & Beyond

Goals of an Attack

- Competition (or Cloning)
  - Specific theft to gain marketplace advantage
- Theft-of-Service
  - Obtaining a service for free that normally costs money
- User Authentication (or Spoofing)
  - Forging a user's identity to gain system access
- Privilege Escalation (or Feature Unlocking)
  - Gaining increased command of a system or unlocking hidden/undocumented features

Trinity
Software & Beyond

Attack Vectors

- Interception (or Eavesdropping)
  - Gain access to protected information without opening the product
- Interruption (or Fault Generation)
  - Preventing the product from functioning normally
- Modification
  - Tampering with the product, typically invasive
- Fabrication
  - Creating counterfeit assets of a product

Trinity
Software & Beyond

Attacking External Interfaces

- Usually a product's lifeline to the outside world
  - Manufacturing tests, field programming/upgrading, peripheral connections
  - Ex.: JTAG, RS232, USB, Firewire, Ethernet
- Wireless interfaces also at risk
  - Ex.: 802.11b, Bluetooth
- Any interface that connects to a third-party may contain information that is useful for an attack
  - Could possibly obtain data, secrets, etc.

Trinity
Software & Beyond

External Interfaces: Backdoors

- Architecture-specific debug and test interfaces
  - Usually undocumented
- Diagnostic serial ports
  - Provides information about system, could also be used for administration
- Developer's backdoors
  - Commonly seen on networking equipment, telephone switches

Trinity
Software & Beyond

Electrical Attacks

- Surface Mount Devices
- Probing Boards
- Memory and Programmable Logic
- Chip Delidding and Die Analysis
- Emissions and Side-Channel Attacks
- Clock and Timing

Trinity
Software & Beyond

Memory and Programmable Logic

- Most memory is notoriously insecure
  - Not designed with security in mind
  - Serial EEPROMs can be read in-circuit, usually SPI or I^2C bus (serial clock and data)
- Difficult to securely and totally erase data from RAM and non-volatile memory
  - Remnants may exist and be retrievable from devices long after power is removed
  - Could be useful to obtain program code, temporary data, crypto keys, etc.

Trinity
Software & Beyond

Memory and Programmable Logic 2

- SRAM-based FPGAs most vulnerable
  - Must load configuration from external memory
  - Bit stream can be monitored to retrieve entire configuration
- To determine PLD functionality
  - Try an I/O scan attack
  - Cycle through all possible combinations of inputs to determine outputs

Trinity
Software & Beyond

Memory and Programmable Logic 3

- Security fuses and boot-block protection
  - Enabled for "write-once" access to a memory area or to prevent full read back
  - Usually implemented in any decent design
  - Might be bypassed with die analysis attacks (FIB) or electrical faults

Trinity
Software & Beyond

Emissions and Side-Channel Attacks

- All devices leak information
  - EMI (electromagnetic interference) from circuits (TEMPEST)
  - Power supply fluctuations
  - Visible radiation from LEDs and monitors
- Can be monitored and used by attacker to determine secret information
- Devices may also be susceptible to RF or ESD
  - Intentionally injected to cause failure

Trinity
Software & Beyond

Emissions Attacks: Power Supply

- Simple Power Analysis (SPA)
  - Attacker directly observes power consumption
  - Varies based on microprocessor operation
  - Easy to identify intensive functions (cryptographic)
- Differential Power Analysis (DPA)
  - Advanced mathematical methods to determine secret information on a device

Trinity
Software & Beyond

Clock and Timing

- Attacks rely on changing or measuring timing characteristics of the system
- Active (Invasive) timing attacks
  - Vary clock (speed up or slow down) to induce failure or unintended operation
- Passive timing attacks
  - Non-invasive measurements of computation time
  - Different tasks take different amounts of time

Trinity
Software & Beyond

Extracting 4096-Bit RSA Key via Sound

- 2013 - Adi Shamir, Daniel Genkin, Eran Tromer
- From standard laptops
- Using standard equipment
- Similar low-bandwidth attack by measuring the electric potential of a computer chassis.
  - Attacker need merely touch the target computer with his bare hand
  - Or get the required leakage information from the ground wires at the remote end of VGA, USB or Ethernet cables

דרכי התמודדות

Trinity
Software & Beyond

Security Through Obscurity

Does **not** work

- Provides a false sense of security to designers/users
- Might temporarily discourage an attacker, but it only takes one to discover it

Trinity
Software & Beyond

General Security Concepts

- Nothing is ever 100% secure
  - Given enough time, resources, and motivation, an attacker can break any system
- Secure your product against a specific threat
  - What needs to be protected
  - Why it is being protected
  - Who you are protecting against (define the enemy)

Trinity
Software & Beyond

Security During Product Development

- Establish a security policy
  - As the "foundation" for design
- Treat security as an integral part of your product's development
- Minimize the elements you need to secure
- Reduce risk to an acceptable level
  - Elimination of all risk is not cost-effective

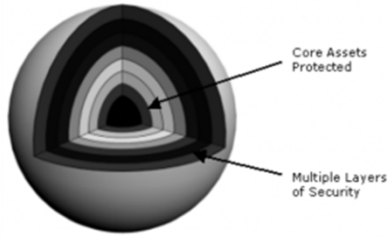
Trinity
Software & Beyond

Security During Development 2

- Implement layered security
- Do not implement unnecessary security mechanisms
  - Each mechanism should support a defined goal
- Costs of a successful attack should outweigh potential rewards

Trinity
Software & Beyond

אספקטים של אבטחה



- במספר רמות
  - דרישות מערכת
  - הנדסת מערכת
  - ארכיטקטורת מערכת
  - תהליכי פיתוח, כולל כלים
  - קידוד מאובטח

Trinity
Software & Beyond

הגנה רב שכבתית

- תיכון מאובטח
- כללי כתיבה מאובטחת - SCA
- אכיפה ברמת הקידוד - SCA
- בדיקות עמידות והקשחה לפלטפורמה - Scan
- בדיקות עמידות והקשחה לתקשורות - Fuzzing
- מיגון התוכנה בפני פריצה, שינוי, והינדוס-הפוך

Trinity
Software & Beyond

Embedded Protection Recommendation

- Anti-tamper
  - In order to trust any application-specific security mechanism, the application logic itself must first be secured
- Inter-component Authentication
  - The interface between vulnerable components is a common area of attack. Components within an application can verify trust in each other
- Trusted Data
  - Structured application data is often the final goal of the attacker. Encode sensitive data, hardening it against illicit access or modification
- … (more)

Trinity
Software & Beyond

Recommendations II

- Secure Application Architecture
  - Designing application security architectures and deploying associated solutions
- Hardware Authentication
  - Where possible


Trinity
Software & Beyond
שאלות? טענות? מענות?
❖ איפה אפשר ללמוד עוד על הנושא?
❖ בואו נדבר ...
תודה !
גיל קיני
Gil @ Trinity.co.il
09-7677880