

# TiViT

## Protecting Communication Networks, Devices, and their Users: Technology and Psychology

Alexey Kirichenko, F-Secure Corporation

ICT SHOK, Future Internet program

30.5.2012

# Outline

TiViT

1. “Security” WP (WP6) overview
  2. Projects, challenges
  3. Theoretical and practical results
  4. One important outcome
-

- **Cross-WP activity in FI 1<sup>st</sup> phase (FI-1)**  
(led by Mikko Särelä of Ericsson, Sasu Tarkoma of TKK)
  - **WP with three activities in FI-2:**
    - Unwanted Traffic
    - Anomaly Detection
    - Trust, Reputation and Management of Credentials  
(1.6.2009 – 31.12.2010, led by Mika Rautila of VTT)
  - **WP with three activities in FI-3:**
    - Botnet Problem
    - Data Analysis for Information Security
    - Understanding and Designing Security Experience  
(1.4.2011 – 31.3.2012)
-

# Partners

TiViT

- Stonesoft
  - Aalto/HIIT, ICS, CSE
  - VTT
  - F-Secure
  - NSN
  - TUT
  - Nokia
  - UH
  - Ericsson
-

- **High diversity in the plans:**
    - Malware and targeted attacks detection and prevention
    - Security for Cloud Computing
    - Manipulation-resistant robust reputation systems
    - Trust between devices and entities in data networks
    - Data access authorization rules and key management
  - **Selected results and advances:**
    - Detecting botnets through anomalous use of network services; identifying Command and Control traffic
    - Security anomaly visualization for a network intrusion detection system, feature selection
    - Call graph-based analysis of executable files
    - UI prototype for collecting feedback and presenting reputation information on widgets and their developers
-

# Moving to FI-3

TiViT

- Due to smaller allocations, fewer directions and partners, narrower focus
  - Greater effort to implementing and testing methods and algorithms:  
“Milestones” defined as prototypes and production system integrations
  - Core areas are:
    - Data analysis for recognizing malicious objects and activities
    - Role of humans in security systems; visualizations
    - Security-related User Experience
-

# WP6 Projects in FI-3

TiViT

- Botnet techniques and botnet characterization and detection approaches (Stonesoft, HIIT)
  - Network-based intrusion detection, role of security officer (NSN)
  - Classification and clustering for detecting malicious files by their static and dynamic features (Aalto/ICS, F-Secure)
  - Study of user perception and experience of security (HIIT, F-Secure)
  - Comparative evaluation of UX for security products (TUT, F-Secure)
  - Security events visualization (Stonesoft)
-

# Fighting Botnets

TiViT

- Analyzing botnet techniques and vulnerabilities used by botnet writers
  - Fingerprints for identifying botnets
    - Based on communication:
      - between bots within a botnet
      - between bots and “Command and Control” (C&C)
      - from bot to drop zone
    - Based on popular exploits
  - Botnet detection techniques
    - DPI of malicious payload or C&C communication
    - Port scanning detection
    - Detecting outgoing spam messages
    - Domain flux analysis (number of DNS requests, mostly failed)
    - Detecting HTTP requests in “click fraud” cases
-



# Network-based Intrusion Detection **TiViT**

- High-level goals:
    - Select “right” features for monitoring and analysis
    - Keep false alarms level low
    - Make analysis results understandable for security officers
    - Ensure that analysis speed scales for high traffic volumes
  - Several Master Thesis works towards the goals:
    - “Traffic analysis for intrusion detection in telecommunications networks” on feature selection for specified threat scenarios
    - “Graphical user interface for intrusion detection in telecommunication networks” on GUI concept and prototype for security anomaly visualization in telco networks
    - “Graph-based clustering for anomaly detection in IP networks” on NodeClustering, a fast and simple anomaly detection method
    - “Selective Flow Distribution for Network-based Intrusion Detection Clusters” on an NIDS cluster load balancing system
-

# UX of Security Products

TiViT

- Comparative evaluation of user experience of several major Internet and mobile security products
    - Development and testing of a process for evaluating security software user experience
    - Usability and security experts were involved in discovering usability problems and suggesting solutions
    - Comparative results were used to find differentiating factors
  - Examples of findings:
    - Warnings in risky situations require understandable words
    - Warning dialogs needed before dangerous changes are applied
    - All evaluated warning flyers diminish too quickly
    - Windows built-in warning appears at the same time
-

# Security Experience

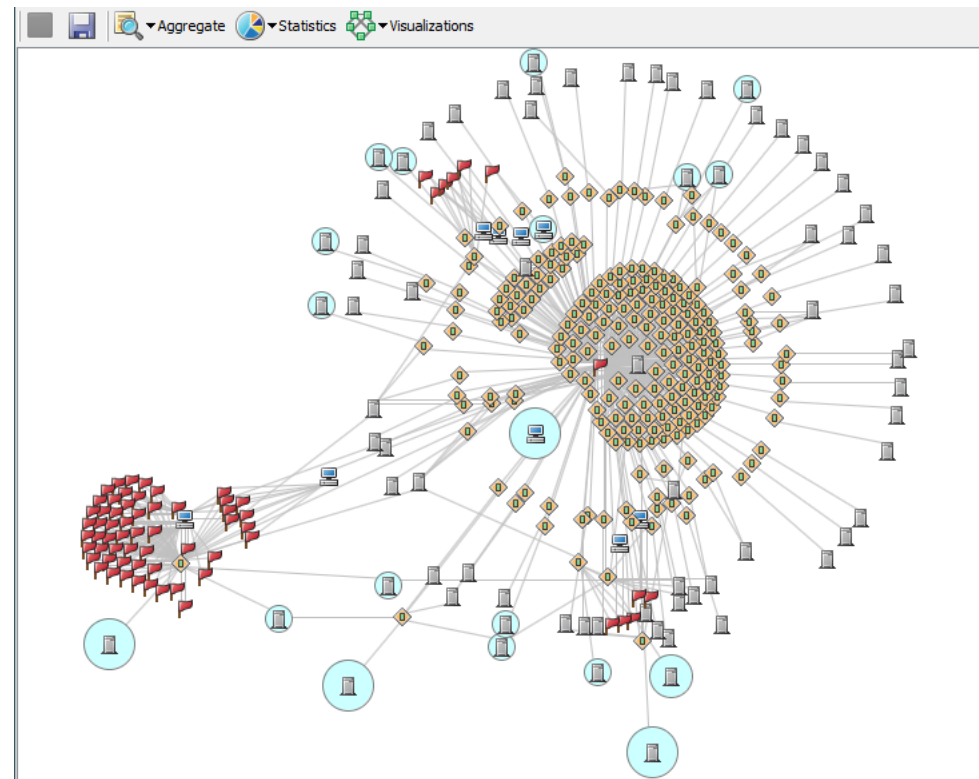
TiViT

- A user study on how end users perceive and experience security in connection with support calls dealing with security issues
    - Run in collaboration with a local teleoperator
    - Individual interviews with support call specialists
    - Focus group with a group of support call specialists
    - Analysis of randomly selected support calls on security
    - Pair interview with support call specialists to check the findings
  - Examples of findings:
    - Security support calls have an essential part in how users try to manage their security
    - Security problems are often confused with device- or network-related ones - problems are often associated with security
    - Constant safety concerns are a major cause for security support calls
-

# Security Events Visualization

TiViT

- Multiple views supported
- Non-deterministic layout algorithm (Kamada-Kawaii)
- Hoovering and zooming
- Drill-in features
- Event normalization
- Aggregation logic for better scalability
- Potential in security device configuring



- As more time went to implementations, the number of publications was modest in WP6 FI-3:
    - Two conference papers published
    - One conference and one journal papers submitted
    - Five University theses (Aalto, TUT)
    - Two conference papers will be submitted in June
-

# Implementations Presented

TiViT

- Classification and clustering methods for identifying malware run in F-Secure's Security Labs  
<http://www.slideshare.net/tivit/tivit-interactive-10185532>
  - Security logs visualization functionality integrated with StoneGate SMC product  
<http://www.slideshare.net/tivit/tivit-interactive-log-visualization>
-

# Observations and Thoughts

TiViT

- Investing in “strategic research” and long-term commitments are hard for many industrial partners
  - Challenging to pursue both “breakthrough results” and “research to lead to new business”
  - Most of work done as two- or even one-party projects  
Working out wider collaborations requires time and effort
  - Relatively short funding periods make it tough to keep key personnel at academic partners
-

# “Data to Security” Ecosystem

TiViT

- An idea of uniting network and device views:
    - Analyzing network traffic, files, scripts, ...
    - Was discussed within the FI program, is becoming a reality now, as a “business pilot ecosystem”
  - All the FI-3 WP6 industrial partners are involved: Stonesoft, NSN, F-Secure
  - New partners: Elisa, EXFO NetHawk
  - Protecting ISP and MNO networks by sharing information from network equipment, end-user devices, and backend analysis systems  
In particular, to deal with botnets
-



# TiViT

Thank you  
[www.futureinternet.fi](http://www.futureinternet.fi)

Alexey Kirichenko, F-Secure Corporation

ICT SHOK, Future Internet program

30.5.2012