Cognitive Security:
A New Approach to Securing Future Large Scale and Distributed Mobile Applications

Wenjing Lou and Nei Kato

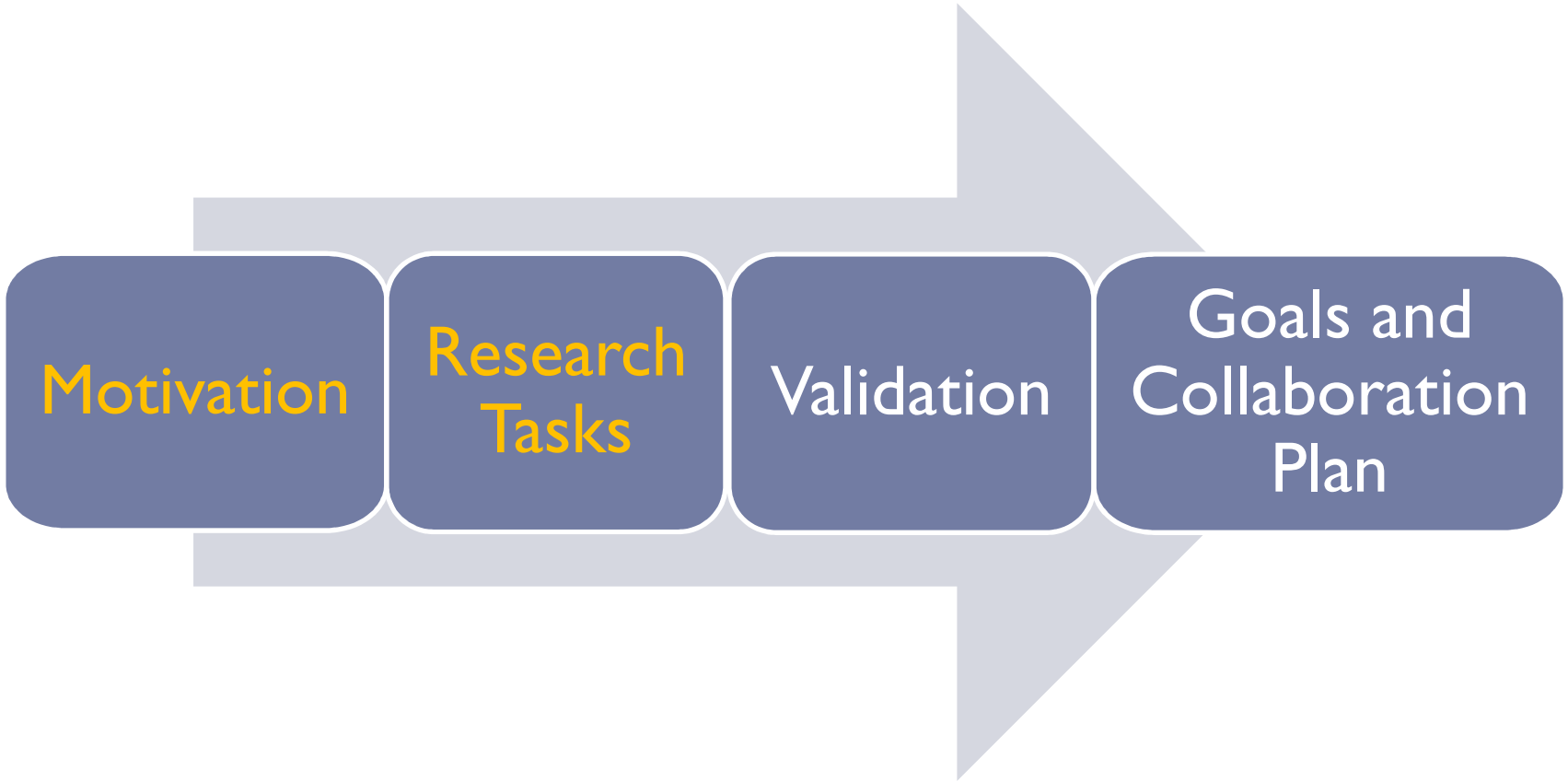
Virginia Polytechnic Institute and State University

Tohoku University

Keio University

NTT Corporation

Outline


Motivation
Research Tasks
Validation
Goals and Collaboration Plan

Security in Wireless Networks

A crucial and challenging problem …

- Open medium, no inherent physical protection
- Devices being "mobile"
- Lack of fixed infrastructure
- Cooperative wireless protocol is more vulnerable
- Dynamic network conditions, hard to distinguish normalcy and anomaly
- Wireless means constant surveillance, privacy is important

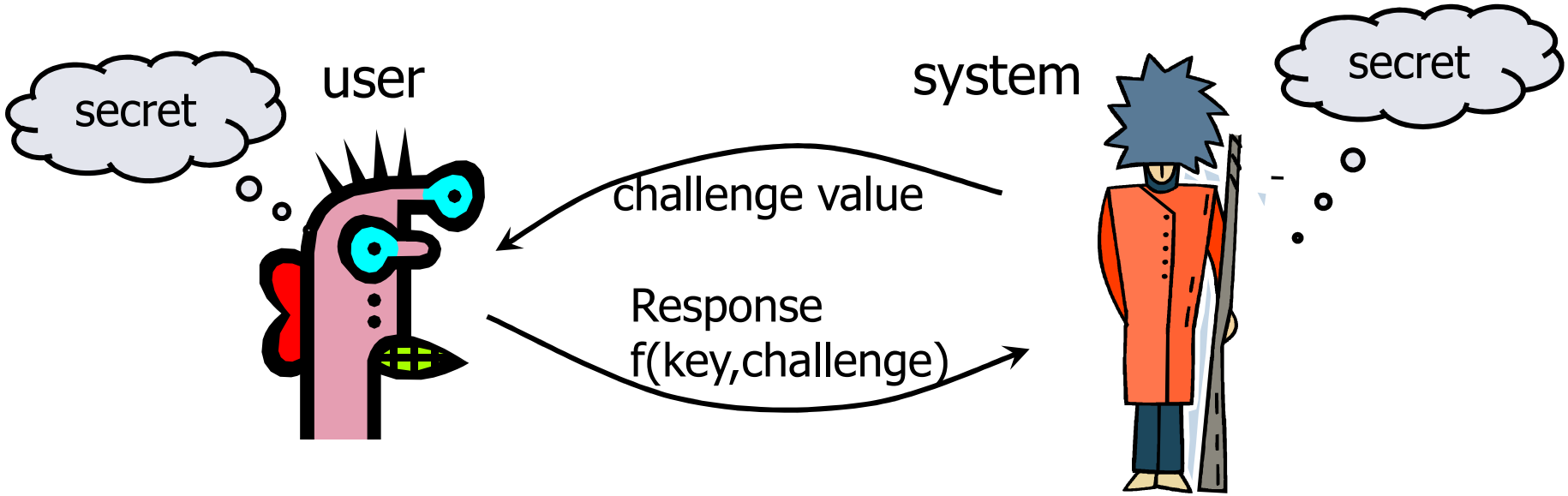
Existing Security Solutions

A huge body of research work …

- Authentication/Authorization
- Confidentiality, Integrity, Available
- Anonymization and privacy
- Secure routing, secure network control and management
- Traffic analysis, location privacy, mobile device information obfuscation
- Intrusion detection
- Mobile security, Android security
- …

Crypto-based Security Solutions

- Conventional cryptography based network security techniques are essential to securing wireless networks.
- Example: Authentication



Rely on prior trust relationship (e.g., shared secret keys, authentic public keys); System is as secure as its key.

Trend toward "Trillions of Objects"

- Explosive deployment of wireless technologies
- Rapid evolution of mobile devices and applications
  - Mobile-connected devices will exceed world's population in 2014
  - Half a billion devices introduced each year
  - Transitioning to smarter mobile devices
  - Projected continued growth in M2M connections

ANDROID

Windows Mobile

Mac OS X

Challenges of "Trillions of Objects"

A pressing security problem in wireless networks …

- Large number of mobile devices and fully distributed control
  - ⇨ loose security management
- Mobile devices are subject to security compromise (loss, stolen, reverse-engineering)
- Insider attacker can easily pass crypto-based security checks

New Approach: Cognitive Security

- Cognitive involves conscious intellectual activity as knowing, perceiving, reasoning or remembering, and is based on or capable of being reduced to empirical factual knowledge
- Cognitive security is to add cognition by exploiting technologies such as machine learning, knowledge representation, network control and management, etc., while solving security problems.
- Instead of relying on pre-configured secrets to authenticate a mobile user/device, we authenticate a user through the properties, patterns or knowledge peculiar to the user that we continuously learned through many interactions we have had with the user.

Scope of Research

- Proximity-based security techniques for location-based services Location
- Cognitive personal verification question (CPVQ)-based security enhancement to mobile user authentication
- Validation and experimentation

Research Agenda and Collaboration Plan

Research Task	Year 1	Year 2	Year 3
Location Tag Construction (Lou, Hou, Kato, Otsuki, Shimizu)	■■■■	■■	
Location Tag Matching and Secret Key Extraction (Lou, Hou, Kato)	■■	■■■■	■■
Social Network Modeling for Security Questions (Lou, Hou, Kato)	■■■■	■■	
PVQs Optimization (Lou, Hou, Kato)	■■	■■■■	■■
Data Collection and Processing (Kato, Nishiyama, Kawamoto, Lou, Hou)	■■■■	■■	
Prototyping and Experimentation (Kato, Otsuki, Shimizu, Lou, Hou)		■■	■■■■

- Monthly video conference calls
- Face-to-face meeting at conferences (e.g. INFOCOM, Globecom, ICC0
- Summer student exchange program

Expected Scientific Outcomes

- Address a pressing security challenge due to the large number of mobile devices under very loose security management
- Explore a novel approach, cognitive security, to enhancing mobile device and application's security
- Deeper understanding of adding cognition to security solutions, basic design principle of cognitive security mechanisms
- Specific solutions to two research problems, i.e. wireless signal based location proof and social network learning based user authentication; research goals presented earlier

Broader Impact

- Data dissemination
  - Software packages: a set of location tag based proximity-based security solutions and a social network based mobile authentication system
  - High quality joint publications between the US and Japan team
- Educational impact
  - Training of graduate students
  - Course module development for courses taught at both institutions
- Industry involvement
  - Tutorial on wireless security offered at Wireless@VT annual symposium which has strong participation from industry and government agencies

Expected achievements of this project

- Providing secured and efficient networks for large scale and distributed mobile applications
- Contributing to the creation and development of industry
- Providing active support for developing human resources of young researchers

THANK YOU