


**Institute for Information Infrastructure Protection**

**Digital Identity Management and Protection**

*Elisa Bertino*  
CS Department and CERIAS  
Purdue University



**I3P Assessable Identity and Privacy Protection Project**

<http://www.thei3p.org>  
Supported by DHS and NIST

## Outline

- Basic Digital Identity Concepts
- Problem of Identity Theft
- Our Solution towards "Establishing and Protecting Digital Identity"
- On-going and Future Work

**I3P** Institute for Information Infrastructure Protection 2

## What is Digital Identity?


Digital Identity:

- Digital representation of the information known about a principal or an organization such as name, address, social security and account numbers, passwords, transaction data, machine tags, IP address etc
- Such data are referred to as *identity attributes*
  - Classified as *strong identifiers* and *weak identifiers*

**I3P** Institute for Information Infrastructure Protection 3

## Digital Identity Basic Concepts

- **Digital Identity:** A set of claims made by one digital subject about itself or another digital subject
- **Claim:** An assertion of the truth of something, typically one which is disputed or in doubt
  - An identifier
  - Knowledge of a secret
  - Personally identifying information
  - Membership in a given group (e.g. people under 16)
  - Even a capability



**I3P** Institute for Information Infrastructure Protection


## Digital Identity Verification

*It deals with verifying that the identity attributes claimed by an individual are owned by that individual*

**I3P** Institute for Information Infrastructure Protection 5

## Identity Theft

IDENTITY THEFT is the use of personally identifying information belonging to one individual by another individual for financial or personal gain.



**I3P** Institute for Information Infrastructure Protection 6

## Threat of Identity Theft: Attack Vectors

|                    |   |
|--------------------|---|
| Technical          | Pharming, Network Sniffing, Database Attacks, Password Cracking |
| Physical           | Dumpster Diving, Trusted Insiders, Theft and Loss               |
| Social Engineering | Phishing, Legal Identity Sources                                |



## Objective – Obtain Individual Identity

| Type               | Attack                   | Description  | Mitigations  |
|--------------------|--------------------------|--|--------------|
| Technical          | Trojan/Keystroke Logging | Spyware/malware placed via hacking, as payload in a virus, or downloaded from an attacker's Web site | 1, 3, 4      |
|                    | Wireless Intercept       | Open access points, AirSnarfing, "Evi Twer"  | 5, 6         |
|                    | Pharming                 | DNS spoofing, DNS cache poisoning, proxy attacks   | 23           |
|                    | Scrape Web Site          | Gather personal data from Web sites to use as verifiers  |              |
|                    | Network Sniffing         | Collect targeted network packets   | 7, 23        |
| Physical           | Theft                    | Stolen mail, wallets/purses, laptops   | 2, 5, 6      |
|                    | Shoulder Surfing         | Direct observation of personal, confidential information   | 2            |
|                    | Dumpster Diving          | Gather discarded documents or hardware (disks)   | 2, 6         |
|                    | Trusted Insiders         | Identify information misused by individuals with access  | 5, 9, 10     |
|                    |                          |  |              |
| Social Engineering | Phishing                 | Luring individuals to reveal confidential information  | 1, 20        |
|                    | Family Members           | Identify information misused by family members   | 2            |
|                    | Legal Identity Sources   | Obtain identity information fraudulently from credit bureaus, government agencies, etc.              | 1, 2         |
|                    | "419" Scams              | Obtain money and/or account information  | 2            |
|                    | Trusted Insiders         | Obtain identity information from service providers (doctors, dentists, lawyers, etc.)                | 1, 2, 21, 22 |

## Objective – Obtain Multiple Identities

| Type               | Attack               | Description   | Mitigations                |
|--------------------|----------------------|---|----------------------------|
| Technical          | Hacking              | Gain privileged access for further attacks and/or data harvesting | 10, 12, 13, 14, 15, 16, 17 |
|                    | Data Attacks         | SQL Injection, XSS attacks  | 7, 16, 19                  |
|                    | Database Attacks     | Login attacks, inference attacks, SQL scanners                    | 1, 5, 15                   |
|                    | Password Cracking    | Acquire admin passwords to servers                                | 1, 15                      |
| Physical           | Theft and Loss       | Backup data, tapes, disks, laptops, etc.                          | 5, 7, 11                   |
|                    | Firewall Breaches    | Connect and map internal network(s)                               | 16, 16                     |
|                    | Dumpster Diving      | Obtain discarded documents, disks, systems, etc.                  | 8                          |
|                    | Trusted Insiders     | Access individuals take data with removable media, e-mail         | 1, 2, 21, 22               |
|                    |                      |   |                            |
| Social Engineering | Gain Physical Access | Computer rooms, server farms, wiring closets, switches, routers   | 1, 2                       |
|                    | Trusted Insiders     | DBAs, employees, contractors, individuals with access             | 1, 2, 21, 22               |
|                    | Phone Requests       | Obtain confidential information to facilitate attacks             | 2                          |

## Defenses and Mitigations

1. Multi-factor authentication
2. User education
3. Anti-virus package(s)
4. Anti-spyware package(s)
5. Encryption
6. Secure configuration
7. Encrypted payload
8. Shredding
9. Enforce need-to-know
10. Access controls and user privileges
11. Policy and enforcement
12. n-tier architecture
13. Real-time monitoring
14. Honey pots/honey nets
15. HIPS (Host Intrusion Protection Systems)
16. NIDS (Network Intrusion Detection Systems)
17. Well-configured firewall(s)
18. Server-side validation
19. Secure coding techniques
20. Browser toolbars
21. Separation of duties
22. Audit controls
23. SSL/TLS

## The VeryIDX project

- A system supporting the privacy-preserving management of identity attributes
- It is based on identity attribute verification policies
- It implements an **identity attributes verification** mechanism based on *aggregated cryptographic zero knowledge proofs*

## Multi-Factor Identity Attribute Verification

It requires additional identity information (like mother maiden name or SSN) as proof to qualify to be the owner of the identity attribute being used (like credit card number)



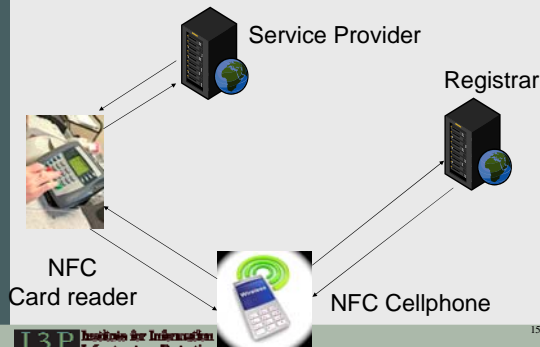
## Privacy preserving Multi-Factor Identity Verification

- **Zero knowledge proof (ZKP)** is an interactive method to prove the possession of a secret without actually revealing it
- **Aggregate ZKP scheme** is used to prove the knowledge of multiple strong identifiers efficiently and reliably without the need to provide them in clear

## Pedersen Commitment – ZK Proving to know how to open

- Public commitment  $c = g^x h^r \pmod{p}$
- Private knowledge  $x, r$
- Protocol:
  1. P (prover): randomly picks  $y, s$  in  $[1..q]$ , sends  $d = g^y h^s \pmod{p}$
  1. V (verifier): sends random challenge  $e$  in  $[1..q]$
  2. P: sends  $u = y + ex, v = s + er \pmod{p}$
  3. V: accepts if  $g^u h^v = dc^e \pmod{p}$

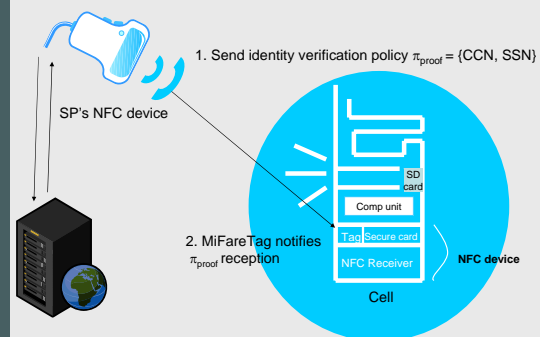
## VeryIDX architecture



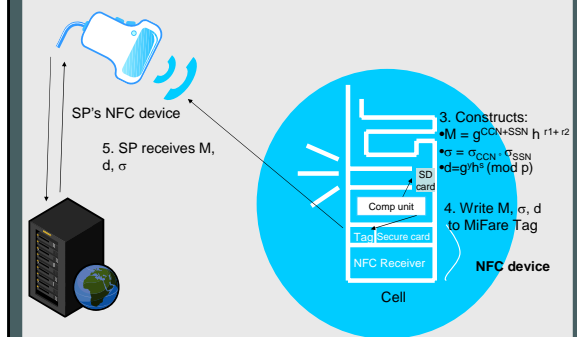
## NFC Nokia mobile phones

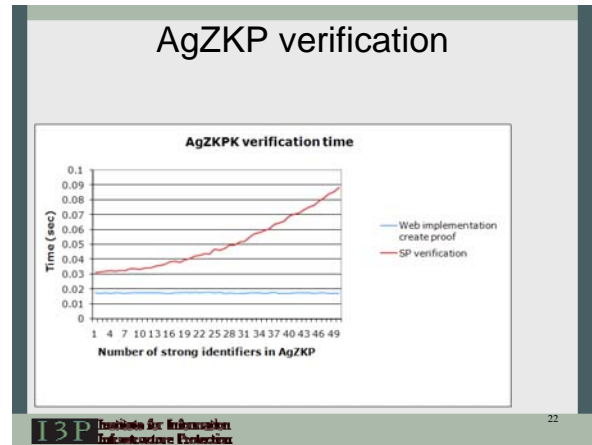
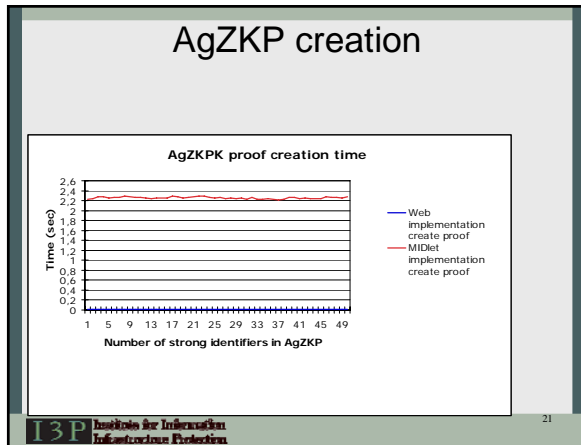
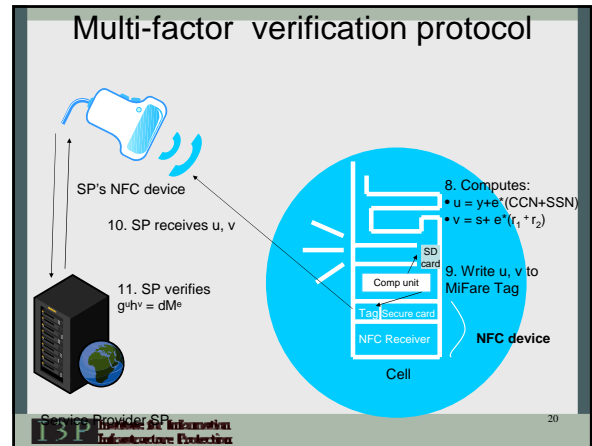
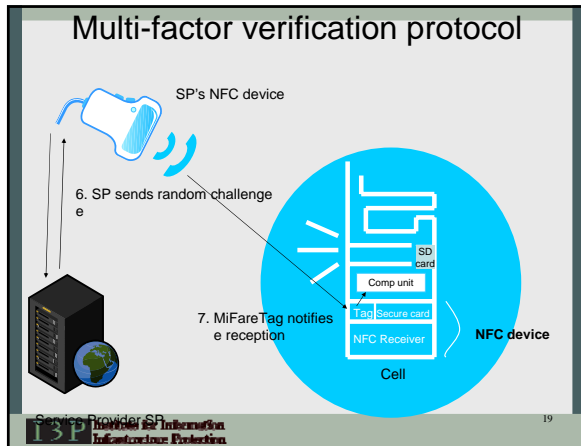
- Java MIDlet to generate AgZKP
- BouncyCastle API to implement AgZKPK
- Code obfuscation to reduce MIDlet size
- Java MIDlet signed by using Nokia Carbide.j tool to access the Mifare Tag
- Identity records stored on the Nokia phone external memory

## Multi-factor verification protocol



## Multi-factor verification protocol





### Interoperability issues in VeryIDX

- *Naming heterogeneity* occurs because clients, service providers and identity providers, very often belong to different domains each using a different vocabulary to denote identity attribute names
- **Solution:** identity attribute name matching protocol based on look up tables, dictionaries and ontology mapping

13P Institute for Information Infrastructure Protection

### On-Going and Future Work

- Use of VeryIDX protocols for identity verification in workflows
- Support for multiple registrars
- Introduction of conditions on identity attributes
- Integration of VeryIDX with CardSpace

13P Institute for Information Infrastructure Protection

## Thank You!

- Questions?
- Elisa Bertino [bertino@cs.purdue.edu](mailto:bertino@cs.purdue.edu)