ATTPS Publication: Trustworthy ICT Taxonomy

Roger Berkley

Trustworthy ICT Taxonomy Research

Cybersecurity technology is a considerably large subdomain of ICT. Technology experts like Gartner have identified at least 94 different technology profiles for secure ICT in their Hype Cycle market research. Likewise, in an attempt to categorize already available Trustworthy technologies, European research project CYSPA identified 21 security technology groups. The SECCORD project has identified 50 independent keywords to classify R&D projects in Trust & Security.

Von Faber and Behnsen introduced the ESARIS Security Taxonomy, which is built to manage the complexity of protecting an industrial ICT service provider. ESARIS is a taxonomy of 31 ICT security standards where each standard comprises several security measures (Faber & Behnsen, 2013).

The National Institute of Communication Technologies (INTECO) provides a framework entitled “Taxonomy of ICT Security Solutions” which includes 13 different types of ICT security products and 8 different types of ICT security services (INTECO, 2010).

Following available similar taxonomy research, and for the need to produce a Trustworthy ICT Taxonomy and the unavailability of a similar construct within our reach project ATTPS decided to take on the task of creating the Trustworthy ICT Taxonomy.

Project ATTPS built the Trustworthy ICT Taxonomy, taking into consideration the available classifications and categorizations. The goal of building a single classification construct (i.e. taxonomy) is to provide a more comprehensive and reasonably complete guideline for clustering Trustworthy ICT and cybersecurity European initiatives to perform various analyses including Research Gap Analysis and Business Impact Analysis performed as part of a Project Portfolio Analysis. ATTPS recognizes the potential use of this taxonomy in other projects, research initiatives and organizations and that is reason for this ATTPS publication.
The Need for a Trustworthy ICT Taxonomy

The need for a Trustworthy ICT taxonomy stems from its role in the Business Impact Analysis and Research Gap Analysis performed as part of the overall portfolio analysis. Figure 1 illustrates this role.

The projects on the project list (item number 1 in Figure 1) constituting the European Trustworthy ICT Innovation Funnel are assigned a project technology classification. Determining a project technology (item 2) relies on direct multilevel input from project leaders or participants. ATTPS collects this data as part of the European ICT project survey. Project respondents select up to three options of classification (focus areas) from the ATTPS Trustworthy ICT Taxonomy (item 0). Additional information to determine a project technology classification is in consideration from CORDIS project descriptions and from European project web sites. Project technology classifications are then mapped to Gartner Hype Cycle (item 3) Technologies for business impact analysis, taking categorical and field technology definitions in consideration for this mapping.

---

1 http://cordis.europa.eu/
Building the ATTPS Trustworthy ICT Taxonomy

For the reasons of achieving a business impact measure, and an effective research gap analysis, project ATTPS took on the task of building the ATTPS Trustworthy ICT Taxonomy for use in the ATTPS project and for general public dissemination.

In this regard, ATTPS took in consideration various sources of information, including the taxonomies presented earlier at the top of this report.

Moreover, and after considering the fitness-for-purpose of various general IT taxonomies, the ACM Computing Classification System\(^2\) was adopted as a starting point. It provided the most comprehensive taxonomy available for modern ICT topics and most suitable for the needs of project ATTPS.

ATTPS, at its own judgement, educated by the available sources of information, extracted a subset of the ACM Computing Classification System as a first step to create the ATTPS Trustworthy ICT Taxonomy.

The ACM subset was then categorized in relation to technological domain and according to technology definitions provided by the available technology definition sources (Gartner IT Glossary\(^3\), TechTarget Computing Glossary\(^4\), Tech Terms Computer Dictionary\(^5\), Techopedia\(^6\)).

Finally, the resulting categorized list was improved through iterated cycles of ATTPS research to identify additional technologies within and closely related to Trustworthy ICT. The input from these research cycles added additional technology categories and fields to the final ATTPS Trustworthy ICT Taxonomy.

The complete ATTPS Trustworthy ICT Taxonomy is presented on the following ages of this publication.

---

\(^1\) http://dl.acm.org/ccs/ccs.cfm?CFID=702965103&CFTOKEN=83959333
\(^2\) http://www.gartner.com/it-glossary/
\(^3\) http://whatis.techtarget.com/
\(^4\) http://techterms.com/
\(^5\) https://www.techopedia.com/
### ATTPS Trustworthy ICT Taxonomy

1. **Trustworthy ICT (Generic)**
   - 0.1 Trustworthy ICT architectures
   - 0.2 Trust frameworks (practical/applicable)
   - 0.3 Trustworthy service design
   - 0.4 Trustworthy service components
   - 0.5 Trustworthy service delivery
   - 0.6 Trustworthy service certification
   - 0.7 Trustworthy service continual improvement mechanisms
   - 0.8 Trustworthy service strategy
   - 0.9 Trustworthy service monitoring
   - 0.10 Validation of trust in trustworthy services

2. **Cryptography**
   - 1.1 Key management
   - 1.2 Public key (asymmetric) techniques
     - 1.2.1 Digital signatures
     - 1.2.2 Public key encryption
   - 1.3 Symmetric cryptography and hash functions
     - 1.3.1 Block and stream ciphers
     - 1.3.2 Hash functions and message authentication codes
   - 1.4 Homomorphic encryption
     - 1.4.1 Fully homomorphic encryption (FHE)
     - 1.4.2 Partially homomorphic encryption (PHE)
   - 1.5 Cryptanalysis and other attacks
   - 1.6 Information-theoretic encryption techniques
   - 1.7 Mathematical foundations of cryptography
   - 1.8 Email Encryption

3. **Formal methods and theory of security**
   - 2.1 Trust frameworks (theoretical)
   - 2.2 Security requirements
     - 2.2.1 Secure by design
   - 2.3 Formal security models
   - 2.4 Logic and verification
     - 2.4.1 Context-aware and content-aware technologies
       - 2.4.1.1 Content aware data loss prevention (DLP)

4. **Security services**
   - 3.1 Authentication
     - 3.1.1 Biometrics
     - 3.1.2 Graphical / visual / Machine-Machine passwords
     - 3.1.3 Multi-factor authentication
     - 3.1.4 Identity proofing services (eID)
   - 3.2 Access control
     - 3.2.1 Attribute Based Mechanisms (Access Control)
   - 3.3 Authorization
3.4 Pseudonymity, anonymity and untraceability
3.5 Privacy enhancing technologies (PET)
   3.5.1 Privacy by design
3.6 Digital rights management
3.6.1 Limited disclosure technology
3.7 Identity Analytics and Intelligence

4. Intrusion/anomaly detection and malware mitigation
   4.1 Malware and its mitigation
   4.2 Intrusion detection systems
      4.2.1 Artificial immune systems
   4.3 Social engineering attacks
      4.3.1 Spoofing attacks
      4.3.2 Phishing
      4.3.3 Other intrusion and anomaly detection and mitigation

5. Security in hardware
   5.1 Tamper-proof and tamper-resistant designs
   5.2 Embedded systems security
      5.2.1 Hardware-based security protocols
      5.2.2 Tokenization
   5.3 Hardware attacks and countermeasures
      5.3.1 Malicious design modifications
      5.3.2 Side-channel analysis and countermeasures
   5.4 Hardware reverse engineering

6. Systems security
   6.1 Operating systems security
      6.1.1 Mobile platform security
         6.1.1.1 Mobile single sign-on
      6.1.2 Trusted computing
         6.1.3 Virtualization and security
   6.2 Distributed systems security
   6.3 Information flow control
   6.4 Denial-of-service attacks
   6.5 Firewalls
   6.6 Vulnerability management
      6.6.1 Vulnerability scanners
      6.6.2 Penetration testing
   6.7 File system security
      6.7.1 File Analysis

7. Network security
   7.1 Security protocols
   7.2 Web protocol security
   7.3 Mobile and wireless security

8. Cloud Security
   8.1 Cloud Data Protection Gateways
   8.2 Cloud Access Security Brokers
89 8.3 Hypervisor Security Protection
90 8.4 High-Assurance Hypervisors
91 8.5 Certification for Cloud Security and Cloud Services
92 8.6 Standardization for Cloud Security
93 8.7 Cloud Governance
94 8.7.1 Accountability for Cloud Services
95 8.7.2 Data Provenance for Cloud Services
96 8.7.3 Audit Mechanisms for Cloud
97 8.7.4 Policy Assurance and Management for Cloud
98 8.7.5 Compliance Mechanisms for Cloud
99 8.7.6 Asset Control and Maintenance for Cloud
100 8.7.7 Monitoring Services & Tools for Cloud
101 9. Cloud Services & Cloud Security Services
102 9.1 Cloud Management Platforms
103 9.1.1 Cloud Service Brokerage
104 9.1.2 Cloud-Based Disaster Recovery Services
105 9.1.3 Cloud Testing Tools and Service
106 9.1.4 Cloud Application Discovery
107 9.2 Virtualization
108 9.2.1 Virtual Machine Resilience
109 9.2.2 Virtual Machine Backup and Recovery
110 9.2.3 Hypervisor / Virtual Machine Monitor
111 9.3 Private Cloud Computing
112 9.3.1 Cloud Computing in Government
113 9.4 Public Cloud Computing
114 9.4.1 European Public Cloud Initiative (Pre-operational)
115 9.4.2 European Public Cloud Service (Operational)
116 9.5 Cloud-Based Security Services
117 9.5.1 SaaS Platform Security Management
118 9.5.2 Security as a Service (SecaaS)
119 9.5.2.1 SecaaS for Enterprise
120 9.5.2.2 SecaaS for Public Social Media
121 10. Database and storage security
122 10.1 Data anonymization and sanitization
123 10.2 Management and querying of encrypted data
124 10.3 Information accountability and usage control
125 10.4 Database activity monitoring
126 10.5 Virtual Directories
127 11. Software and application security
128 11.1 Software security engineering
129 11.2 Web application security
130 11.3 Social network security and privacy
131 11.4 Domain-specific security and privacy architectures
132 12. Large-scale system security
133 12.1 Physically-coupled system security (tight coupling)
12.1.1 Systems of systems security (Tightly-coupled)
12.2 Loosely-coupled system security
   12.2.1 Service oriented architecture security
   12.2.2 Message-based service integration security
   12.2.3 Systems of systems security (Loosely-coupled)
13. Human and societal aspects of security and privacy
   13.1 Economics of security and privacy
      13.1.1 Economics of trust in information technology
   13.2 Social aspects of security and privacy
      13.2.1 Usability in security and privacy
      13.2.2 Personalization of security and privacy
      13.2.3 Flexible localization (optional localization)
   13.3 Privacy protections
      13.3.1 Internet Reputation Management (Enterprise)
      13.3.2 Persona management (individuals)
   13.4 Regulation for security & privacy
   13.5 Standards Development for security & privacy
   13.6 Software and System security in Government
References


National Institute for Communications Technologies INTECO. (2010). TAXONOMY OF ICT SECURITY SOLUTIONS.