Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 183 (2017)

Heft: 5

Artikel: Einflüsse von Quantum Computing auf die "Internet of Things"-Security

Autor: Gribi, Klaus

DOI: https://doi.org/10.5169/seals-681617

Einflüsse von Quantum Computing auf die «Internet of Things»-Security

Das Internet of Things (IoT) verbreitet sich immer mehr, wegen seiner rasanten Entwicklung gerät die Informationssicherheit ins Hintertreffen. Neue Technologien wie Quantum Computing verschärfen die Situation zusätzlich. Bewährte Sicherheitsmechanismen wie Verschlüsselung bieten künftig nicht mehr genügend Sicherheit, sobald der erste Quantum Computer verfügbar sein wird.

Klaus Gribi, Dominique Brack

Das Internet of Things (IoT) lässt sich der Operationssphäre Cyber-Raum zuordnen und erfasst durch seine umfassende Verbreitung sämtliche Wirtschaftssektoren, inklusive Armee und Rüstungsindustrie. Drohnen, intelligente Helmvisiere, tragbare Computer (Wearables) für Führungsinformationssysteme, dedizierte IoT-Netzwerke, vernetzte Medizingeräte und selbstfahrende Fahrzeuge werden die moderne Gesellschaft in einem nie dagewesenen Ausmass beeinflussen. Verschiedene Auswirkungen lassen sich bereits heute im öffentlichen Raum feststellen: Videokameras zeichnen das Geschehen an öffentlichen Plätzen auf und mit anonymen Mobilfunknetz-/Smartphone-Informationen (WLAN- und GPS-Positionsinformationen) lassen sich Bewegungsströme darstellen. Diese Situation wird durch die Vernetzung der einzelnen Things weiter verschärft, es entsteht eine neue Risikolandschaft, die es zu analysieren und verstehen gilt. Das US Army Research Laboratory zeigt im Report «Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report»[1] die künftige Problematik umfassend auf.

IoT und Informationssicherheit

Die Informationssicherheit kann heute im IoT-Umfeld in bewährter Manier gewährleistet werden. Die bisherigen technischen Massnahmen wie z.B. Authentisierung, Verschlüsselung, Aufzeichnung (Logging) und Härtung gelangen auch bei IoT zur Anwendung. Die permanente Aktualisierung der Things im Sinne eines Vulnerability-/Patch-Managements wird jedoch eine besondere Herausforderung darstellen, da sich die vielen Millionen Things nicht analog traditioneller IKT-Systeme aktualisieren lassen. Leider muss zum heutigen Zeitpunkt festgestellt werden, dass viele Hersteller und Administratoren von IoT-Geräten die grundlegendsten Sicherheitsvorkehrungen missachten und dadurch implizit Cyber-Attacken ermöglichen. Die Schadsoftware Mirai nutzte im Oktober 2016 eine zwölf Jahre alte Verletzlichkeit aus und befiel rund zwei Millionen IoT-Geräte, welche dadurch Teil eines Bot-Netzwerkes wurden. Das Bot-Netzwerk wurde anschliessend für die bisher weitreichendste DDoS-Attacke[2] (Distributed Denial of Service) eingesetzt.

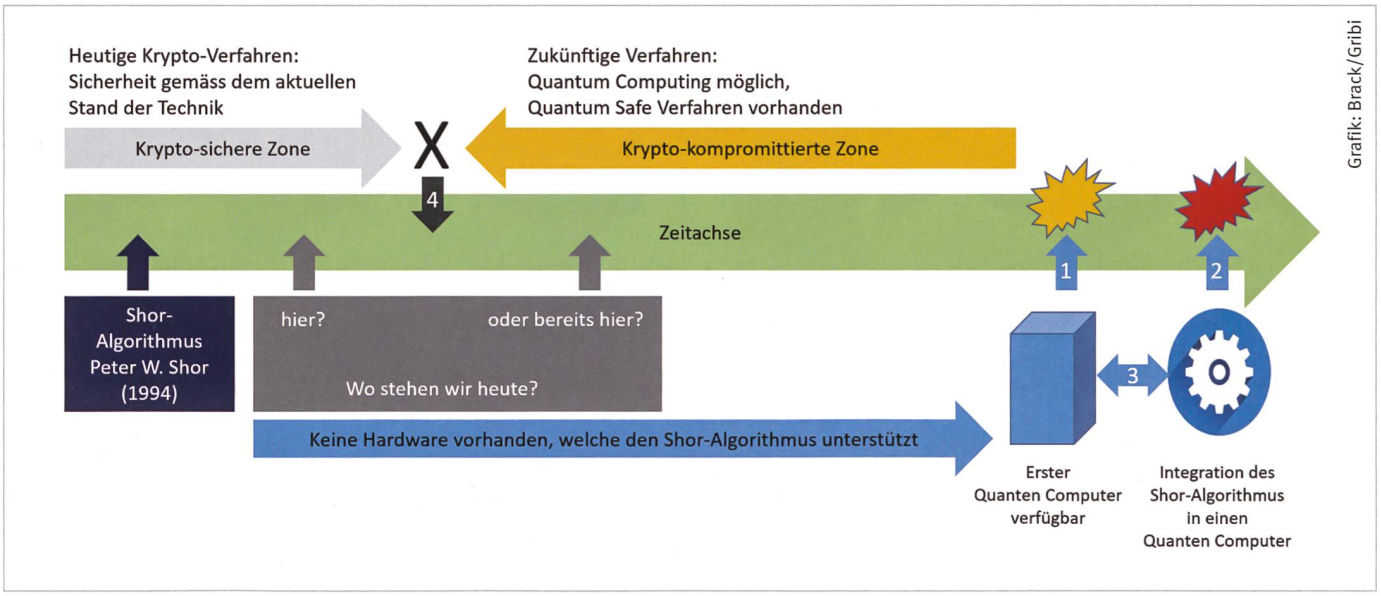
Dieser Situation kann durch spezifische Risikoanalysen begegnet werden, welche das bedarfsgerechte Umsetzen von mitigierenden Massnahmen erlauben. Des Weiteren gibt es verschiedenste OSINT-Informationen (z.B. Richtlinien, Handbücher, Checklisten), welche für die sichere Entwicklung und den sicheren Betrieb der Things herangezogen werden können. An dieser Stelle sei ferner der Hinweis auf die internationale Organisation «Cloud Security Alliance» erlaubt, welche detaillierte kostenlose Grundlagendokumente[3] zu IoT-Security publiziert. Glücklicherweise kann zudem festgestellt werden, dass der Chef Cyber Defense der Armee, Oberst i Gst Gérald Vernez, die Gefahren von IoT bereits vor geraumer Zeit erkannt hat und in seinen Referaten kritisch auf die IoT-Entwicklungen hinweist.

Verschlüsselte Übertragung von Informationen

Die einzelnen Things werden mit unterschiedlichsten Netzwerk-Technologien (z.B. WLAN, Low Power Netzwerke, Near Field Communication) vernetzt, damit sie untereinander kommunizieren können. Diese Vernetzung stellt einerseits

Die technologische Entwicklung im Kontext von IoT beeinflusst auch Sicherheitsbelange im Alltag der Armee, speziell einer Milizarmee. Als Chef des militärischen Teils der Informations- und Objektsicherheit (IOS) bin ich mir bewusst, dass die Angehörigen der Armee bewusst oder unbewusst zivile Gegenstände in das militärische Umfeld mitbringen, die die Informationssicherheit kompromittieren können. Solche Gegenstände müssen nicht zwangsläufig IT-Geräte sein. In Zukunft sind dies auch mit vernetzten IT-Komponenten versehene Kleidungsstücke, Armbanduhren, Brillen oder ähnliche Gegenstände.
Es braucht neue Sicherheitskonzepte, um diesen Gefährdungen zu begegnen. Die daraus abgeleiteten Massnahmen müssen zwingend auch eine umfassende und wiederkehrende Sensibilisierung für das Thema IoT und deren Gefährdungen und eine Verhaltensschulung umfassen. Die Risiken lassen sich nicht einfach mit technischen Massnahmen minimieren. Bei der Sensibilisierung und Verhaltensschulung geht es nicht darum, IoT schlecht darzustellen oder gar die Entwicklung in Richtung IoT zu behindern, sondern um einen bewussten Umgang mit dieser Technologie und einen sinnvollen Einsatz oder Verzicht während des Militärdienstes.
Bei der Sensibilisierung und Verhaltensschulung kann der Astt 160 wertvolle Arbeit leisten, indem er Schulungsgrundlagen vorbereitet, Schulungskampagnen unterstützt und im Rahmen der Truppenkontrollen die Kader und Mannschaft sensibilisiert.

Oberst Peter Christen, Chef Astt 160 – IOS



Auswirkung Quantum Computing.

den Hauptnutzen, aber andererseits gleichzeitig auch eine Hauptgefahr von IoT dar, da Informationen fast beliebig unter den Things ausgetauscht werden können. Damit die Vertraulichkeit dieser Informationen gewährleistet werden kann, werden sie während der Übertragung normalerweise verschlüsselt (data in transit). Zu diesem Zweck wird die Verschlüsselungstechnologie (Verschlüsselungsmechanismen und -protokolle) gemäss dem aktuellen technischen Stand eingesetzt. Werden diese Kryptosysteme korrekt parametrisiert und implementiert, können Informationen während der Übertragung mit grosser Wahrscheinlichkeit ausreichend geschützt werden. Wichtig dabei ist insbesondere, die zur Verschlüsselung genutzten kryptografischen Schlüssel in der eigenen Hand zu behalten. Die Verschlüsselung wird heute auf verschiedenen Netzwerkebenen sowie auf der Applikationsebene eingesetzt. Beispiele: Das Führungsnetz CH verschlüsselt Informationen auf Netzwerk-Ebene (data in transit), die Sicherheitssoftware SecureCenter der IOS (www.aios.ch) dient der Dateiverschlüsselung auf Applikations-Ebene (data at rest), E-Mails können bei Bedarf digital signiert und verschlüsselt übertragen werden. Doch weder die technischen Möglichkeiten der Geheimdienste[4] noch die technologischen Weiterentwicklungen stehen still. Im Bereich der technologischen Weiterentwicklungen stellt Quantum Computing[5] für die heutige Verschlüsselungstechnologie eine ernstzunehmende Bedrohung dar, welche nachfolgend aufgezeigt wird.

Quantum Computing – wie aus verschlüsselten Informationen Postkarten werden

Wie situiert sich Quantum Computing in Bezug auf die IoT-Risiken? Es wird erwartet, dass die zwei meist verbreiteten Public Key Kryptosysteme RSA und Elliptic Curve Cryptography (ECC) künftig durch Quantum Computer kompromittiert werden können. RSA und auch ECC werden zum Beispiel bei Transport Layer Security (TLS) eingesetzt. TLS wird als sicheres Transport-Protokoll eingesetzt, damit Informationen zwischen den vernetzten Things verschlüsselt übertragen werden können. In Web Browsern (Internet Explorer, Firefox etc.) wird TLS für das verschlüsselte Übertragen von Informationen eingesetzt (Secure Hypertext Transfer Protocol, https), z. B. beim E-Banking. Der erste verfügbare Quantum Computer wird solche gängige und sichere Übertragungsprotokolle aufbrechen können, der Verlass auf diese Protokolle wird nicht mehr gegeben sein. Sichere Kommunikationsketten werden künftig unsicher, von der Quelle bis zum Ziel. Zusätzlich verschärfend wirkt sich aus, dass auch die auf Speichermedien verschlüsselten Informationen (z. B. SecureCenter Chiffrate) selbst und nicht nur die geschützte Kommunikationsübertragung betroffen sind. Dadurch ergeben sich gänzlich andere Bedrohungsszenarien: Ein Staat kann heute verschlüsselte Informationen in seinem Interessensgebiet speichern und vorhalten, damit diese – bei späterer Verfügbarkeit eines Quantum Computers – entschlüsselt werden können. Nicht nur die Vertraulichkeit selbst, sondern auch die Integrität und die Authentizität der übertragenen und gespeicherten Informationen kann nicht mehr gewährleistet werden. Veränderte oder kompromittierte Informationen können nicht mehr detektiert werden. Somit entsteht nebst den rein technischen Problemen auch ein riesiges Schadenspotential in Bezug auf die regulatorischen Anforderungen und damit bezüglich Compliance.

«Der Astt 160 – IOS leistet bezüglich Sicherheits-Sensibilisierung der Truppe wertvolle Arbeit.»

Quantum Computing wird im Zusammenhang mit dem Shor-Algorithmus[6], welcher 1994 durch Peter W. Shor entwickelt wurde, die Public Key Kryptosysteme nachhaltig verändern. Die obenstehende Grafik «Auswirkung Quantum Computing» verdeutlicht den Kontext.

Bis anhin gibt es scheinbar keinen Quantum Computer, der diesen Algorithmus rechnen kann respektive unterstützt. Auf heutigen Rechner-Systemen wird der Shor-Algorithmus nicht eingesetzt, da die Rechenleistung nicht ausreichend ist. Zwei Ereignisse sind demnach von zentraler Bedeutung: 1. Wann wird der erste Quantum

Computer zur Verfügung stehen (Punkt 1 in der Übersicht)? 2. Wann wird der Shor-Algorithmus auf dem ersten Quantum Computer einsetzbar sein (Punkt 2)? Der Zeitraum zwischen dem Erscheinen des ersten Quantum Computers und bis zur Integration des Shor-Algorithmus wird als kurz eingeschätzt (Punkt 3). Diese Integration bestimmt den Zeitpunkt X (Punkt 4). Wenn der Zeitpunkt X erreicht ist, befindet man sich in der krypto-kompromittierten Zone, in welcher die verschlüsselte Kommunikation (data in transit) und die verschlüsselten Daten (data at rest) kompromittiert werden können. Mit anderen Worten sollten nach dem Zeitpunkt X nur noch sogenannte Quantum Safe Kryptosysteme eingesetzt werden und damit das Quantum Safe Computing ermöglichen. Das grösste Problem stellt die Standortbestimmung dar: Befinden wir uns aktuell noch in der krypto-sicheren oder bereits in der krypto-kompromittierten Zone? Den aktuellen Stand der Dinge halten insbesondere interessierte Staaten geheim. Als Konsequenz daraus entsteht ein gewisser Zeitdruck und Handlungsbedarf.

Ist das Ganze nicht nur eine Eintagsfliege, mit anderen Worten eine überspitzte Risikosicht, welche von Informationssicherheits-Fanatikern kreiert wird? Die Relevanz des obengenannten Themas kann mittels öffentlichen Quellen (OSINT) erhärtet und bestätigt werden (z. B. qualifizierte Fachartikel, initiierte Projekte, getätigte Investitionen von Staaten und technischen Institutionen, Firmengründungen). Viele Quellen messen dem Thema höchste Relevanz bei, nachfolgend werden nur zwei Quellen aufgeführt: Die National Security Agency (NSA) hat ein FAQ (Frequently Asked Questions) zu diesem Thema publiziert[7]. Im FAQ wird erläutert, welche Kryptosysteme für Data in transit im Umfeld von Quantum Computing eingesetzt werden sollen. Weiter erstellt die Internet Engineering Task Force (IETF ist eine offene internationale Gemeinschaft von Netzwerkdesignern, professionellen Anwendern und Herstellern, die zur Entwicklung des Internet und dessen reibungslosem Betrieb beitragen), einen Draft[8], wie «Quantum Safe»-Algorithmen eingesetzt werden können.

Konklusion und Lösungsansätze

Das Bewusstsein bezüglich IoT-Security und Quantum Computing muss zeitnahe weiter gestärkt werden. Insbesondere muss einerseits eine umfassende Risikoanalyse zu diesen Themen erstellt werden, andererseits empfiehlt es sich, bereits heute die möglichen Auswirkungen von Quantum Computing auf die in der Armee und Verwaltung eingesetzten Kryptosysteme im Auge zu behalten. Die Armee setzt die heutigen gängigen Kryptosysteme in vielen Anwendungsgebieten ein, z. B. in Netzwerken, bei Übermittlungssystemen, bei Data at rest oder bei Data in transit. In welcher Art und Weise diese Anwendungsgebiete künftig mittels Quantum Safe Computing weiterhin gesichert werden können, muss unbedingt untersucht werden. Aus Sicht der Informationssicherheit sind die möglichen technischen, organisatorischen und administrativen Anforderungen und mitigierenden Massnahmen festzustellen. Die betroffenen VBS-Stellen wie z. B. die Integrale Sicherheit (IOS), die Führungsunterstützungsbasis (FUB) und Cyber Defense müssen die bedarfsgerechten Lösungen für den Cyber-Raum zeitgerecht bereitstellen. Es stellt sich die Frage, ob allenfalls die bestehende «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» in Bezug auf Quantum Safe Computing situativ angepasst werden muss. ■

1 https://www.hsdl.org/?abstract&did=768193
2 https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
3 https://cloudsecurityalliance.org/group/internet-of-things/
4 http://www.zdnet.com/article/how-the-nsa-and-your-boss-can-intercept-and-break-ssl/
5 https://de.wikipedia.org/wiki/Quantencomputer
6 https://de.wikipedia.org/wiki/Shor-Algorithmus
7 https://www.iad.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm
8 https://tools.ietf.org/html/draft-whyte-qsh-tls13-03

Oberstlt
Klaus Gribi
Astt 160 IOS, USC Info Sich
Senior Security Consultant
Swisscom (Schweiz) AG
3000 Bern

Dominique Brack
Senior Security Consultant
Swisscom (Schweiz) AG
3000 Bern