

December 2011



Newsletter

Our Mission: Provide our members opportunities for career development and networking with peers. Advance and promote the profession by creating awareness of the skills and abilities of IT audit and security Professionals.

Greetings Utah Chapter members,

For December, we will have Dr. Conan Albrectht from Brigham Young University at our monthly luncheon on December 15, 2011 speaking on the topic "Picalo, an introduction to an Open-source Data Analysis Library and Platform." Here is a brief intro about Conan and his topic.

Picalo is a data analysis application, with focus in fraud detection and data retrieved from corporate databases. Professor Connan Albrecht created it as the foundation for an automated fraud detection system that is free and open source. He has used in financial services environments world-wide.

Picalo is currently focused on data analysis for fraud and corruption detection. However, it is an open framework that could actually be used for many different types of data analysis: network logs, scientific data, any type of database-oriented data, and data mining.

Connan Albrecht is an Associate Professor of Information Systems at Brigham Young University. He teaches intermediate and enterprise Java programming to students in the ISys Core. His research topics include computer-aided fraud detection, group support systems, and ecommerce architectures.

When Professor Albrecht is not teaching, researching, or developing, he spends time with family, mountain biking, reading, fishing, hunting, snowmobiling, and skiing.

You can register for this event on the ISACA website (<http://www.isaca-ut.org/utahevents.html>).

Thanks
Josh Taylor
Newsletter Editor

Monthly Professional Training

Date: Thursday, December 15, 2011

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Conan Albrecht

Topic: "Picalo, an introduction to an Open-source Data Analysis Library and Platform"

Cost: \$20 for members and \$15 for students, \$25 for non-members

CPE: 1 Credit

Register at: <http://www.isaca-ut.org/utahevents.html>

Monthly Training Registration

The cutoff time period to sign up for the professional lunch meeting is the Tuesday before the monthly Thursday meeting. If you sign up after noon on Tuesday, you may or may not have a guaranteed seat. Since the rooms at the Lion House are small we have to give them a hard count by Tuesday at noon to reserve a room.

Earning CPE

ISACA e-Symposium

If you are in need of CPE credits, an easy way to earn them is by participating in an ISACA e-Symposium. These are free online web casts and you can earn 3 CPE credits. For further details, go to: www.isaca.org/webcasts

There is no limit to the number of e-Symposiums or on-line quizzes that you can take to help fulfill your CPE requirements. If you have any questions concerning CPE credits please email the following: certification@isaca.org and they will answer your questions.

Monthly Article

QR Vulnerabilities

QR codes (Quick Response) are those square bits of two dimensional barcode ubiquitous in magazines, IT products, automobile inventories, and books now often seen in street advertising. They were invented by the Japanese and are encoded in both vertical and horizontal directions holding more data than traditional bar codes. Data is accessed by capturing a photograph of the code using a camera, usually a smartphone and processing the image through a QR reader. In some sectors QR codes have already overtaken traditional barcodes that can only hold 20 characters where QR codes can hold up to 7,089 characters. And if measured on par, QR codes more appealing because they can hold approximately roughly 300 times the data in about the same space. QR codes don't need to be read from one particular angle since they can be scanned regardless of their positioning.

Initially they were used by manufacturers to track parts, but quickly businesses saw a variety of different uses for them. The most popular use for QR codes is in telecommunications where smartphones are the prevalent driver for their popularity. QR codes appear to be a tool to communicate URLs and other data to users through media most often like magazines, newspapers, business cards, public transport vehicles or other means that might accept printed QR codes as carriers in advertisements for online products. For auditors, remember that QR codes must be considered media so if an organization has a policy of "no outside" media being introduced into the organization's systems, this must include QR codes.

One might distinguish two different threat modes for manipulating QR codes. It is possible for an attacker to invert any module by changing it from either black to white or the reverse. Secondly, an attacker might change only the white modules to black but not the reverse, meaning not the black to white.

The easiest approach to attack an existing QR code is by generating a sticker where manipulating the QR code in the same style as the original QR code and position it over the code in the original QR code. This requires a printer and design applications for the device. This is basically a trivial attack and one that is easily mounted. Defeating this attack depends on backend input application safety checks. Prudent SDLC administration should have these control steps in place as part of their development procedure. Auditors must ascertain that appropriate controls are in force making attack vectors infeasible through QR inputs.

QR codes contain a lot of information including Meta information, masking and source encoding. Masks are used to generate QR codes with black and white distributions of contrast ratios close to 50-50. This has optimal contrast of the picture helping devices decoding it. There are several possible source encodings specified for the data contained in the code maximizing the capacity and increasing its complexity.

Changing its mode indicator gives the encoded information new meaning (Yep, this means a buffer overflow!) when considering an 8-bit byte mode instead of other modes or alphanumeric mode instead of numeric ones. Launching SQL injections become feasible at this point as attack vectors using QR codes.

As QR codes become the de facto means of encoding information it is likely that the majority of software developers will not treat the encoded information as a possible insecure input. QR codes can be altered to change the meaning of the intended encoded information allowing attackers to take control of a system. Depending on the programs that process the inputs, it could mean that logistics, public transportation, assembly line, banking, advertising, or reader software inputs allow unintended access to backend data applications.

QR codes can be currently manipulated allowing vectors through:

SQL injection

Command injection

Fraud (Tricking the system into processing an item as a cheap item when in fact it is an expensive item.)

Alan B. Sternecker, CISA, CISM, CFE, CISSP is a consultant and author of Critical Incident Management, ISBN: 084930010X, published by CRC Press, www.crcpress.com. He has written numerous articles and regularly lectures regarding fraud and computer systems security auditing. He can be reached at absterneckert@yahoo.com

Board of Directors and Officers

Can be found on <http://www.isaca-ut.org/administration.html>

The views and opinions contained in this publication are solely those of the authors, and do not necessarily represent or reflect the view or opinions of the Utah Chapter. In the event you have any questions concerning an article, you may wish to contact the author directly.